Příloha zadávací dokumentace č. 2

Smlouva o dodávce, implementaci a technické podpoře řešení pro zvýšení kybernetické bezpečnosti informačních a komunikačních systémů

(dále jen „***Smlouva***“)

uzavřená ve smyslu § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“), za přiměřeného použití § 2358 a násl. občanského zákoníku, § 2586 a násl. ve spojení a § 2631 a násl. občanského zákoníku, a dle zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským (dále jen „autorský zákon“)

mezi těmito smluvními stranami:

Objednatel:	**Vyšší odborná škola zdravotnická Brno, příspěvková organizace**
se sídlem:	
zastoupen:	
IČO:	00637980
Bankovní spojení:	
Číslo účtu:	

(dále také jako „***Objednatel***“ či „***Nabyvatel***“)

Dodavatel:	**Aricoma Systems a.s.**
se sídlem:	
zastoupen:	
Zapsán OR:	Vedeného Krajským soudem v Ostravě oddíl B, vložka 11012
kontaktní osoba ve věcech smluvních:	
kontaktní osoba ve věcech technických:	
IČO:	04308697
DIČ:	CZ04308697
Bankovní spojení:	
Číslo účtu:	

(dále také jako „***Dodavatel***“ či „***Poskytovatel***“)

(společně jako „***smluvní strany***“ či jednotlivě jako „***smluvní strana***“)

uzavřely tuto Smlouvu na základě výsledku zadávacího řízení na veřejnou zakázku s názvem „**Zajištění kybernetické bezpečnosti VOŠZ Brno, příspěvková organizace - opakovaná“.**

I. ÚVODNÍ USTANOVENÍ

1. Objednatel zahájil veřejnou zakázku s názvem „Zajištění kybernetické bezpečnosti VOŠZ Brno, příspěvková organizace - opakovaná“, přičemž nabídka Dodavatele byla vybrána jako nejvhodnější.

2. Na základě této Smlouvy má Dodavatel ve prospěch Objednatele dodat řešení pro zvýšení kybernetické bezpečnosti Objednatele, provést jeho implementaci do infrastruktury Objednatele, a zajistit technickou podporu tohoto řešení, a to za podmínek dále uvedených v této Smlouvě a jejích přílohách.

3. Závazek mezi smluvními stranami založený touto Smlouvou se řídí zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“), a zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „autorský zákon“).

4. Tato Smlouva je uzavřena na základě výsledku zadávacího řízení vedeného podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „***ZZVZ***“). Jednotlivá ustanovení této Smlouvy musí být vykládána v souladu se zadávacími podmínkami uvedenými v zadávací dokumentaci veřejné zakázky, vč. jejich příloh, a v souladu s nabídkou Dodavatele podanou v rámci zadávacího řízení veřejné zakázky.

5. Účelem uzavření Smlouvy je dodávka komponent softwarové (SW) a hardwarové (HW) infrastruktury a jejich instalace, implementace a vzájemná integrace na stávající informační systémy Objednatele za účelem zvýšení kybernetické bezpečnosti Objednatele, a posílení schopnosti odolávat vnějším kybernetickým hrozbám.

6. Na realizaci projektu byla přislíbena finanční podpora Národního plánu obnovy. Dodavatel je povinen poskytnout objednateli veškerou součinnost tak, aby financování projektu nebylo ohroženo. Dodavatel je povinen uchovávat veškerou dokumentaci související s realizací projektu včetně účetních dokladů minimálně do konce roku 2036.

II. PROHLÁŠENÍ SMLUVNÍCH STRAN

1. Dodavatel prohlašuje, že je plně způsobilý k řádnému a včasnému provedení předmětu této Smlouvy, že se řádně seznámil s rozsahem a povahou předmětu Smlouvy, a to takovým způsobem, že jsou mu známy veškeré relevantní technické, kvalitativní a jiné podmínky nezbytné k jeho realizaci, a že disponuje takovými kapacitami a odbornými znalostmi, vlastním technickým vybavením a zázemím, které jsou nezbytné pro realizaci předmětu Smlouvy za dohodnuté smluvní ceny uvedené v této Smlouvě, a to rovněž ve vazbě na jím prokázanou kvalifikaci pro plnění veřejné zakázky.

2. Dodavatel je oprávněn plnit předmět této Smlouvy pouze prostřednictvím svých zaměstnanců nebo osob uvedených v seznamu poddodavatelů (příloha č. 3 této Smlouvy).

3. Dodavatel dále prohlašuje, že není v úpadku ani ve stavu hrozícího úpadku, a že mu není známo, že by vůči němu bylo zahájeno insolvenční řízení. Rovněž prohlašuje, že vůči němu není v právní moci žádné soudní rozhodnutí, případně rozhodnutí správního, daňového či jiného orgánu na plnění, které by mohlo být důvodem zahájení exekučního řízení na majetek Dodavatele a že takové exekuční řízení nebylo vůči němu zahájeno.

4. Smluvní strany prohlašují, že identifikační údaje smluvních stran uvedené v této Smlouvě odpovídají aktuálnímu stavu, a že osobami jednajícími při uzavření této Smlouvy jsou osoby oprávněné k jednání za smluvní strany. Jakékoliv změny předmětných údajů, jež nastanou v době po uzavření této Smlouvy, jsou smluvní strany povinny bez zbytečného odkladu písemně sdělit druhé smluvní straně.
5. V případě, že se kterékoliv prohlášení některé ze smluvních stran podle tohoto článku Smlouvy ukáže být nepravdivým, odpovídá tato smluvní strana za škodu a nemajetkovou újmu, která nepravdivostí prohlášení nebo v souvislosti s ní druhé smluvní straně vznikne.
6. Dodavatel a Objednatel se zavazují k vzájemné součinnosti za účelem plnění předmětu této Smlouvy.

III. PŘEDMĚT SMLOUVY

1. Předmětem této Smlouvy je závazek Dodavatele dodat komponenty softwarové (SW) a hardwarové (HW) infrastruktury, provést jejich instalaci, implementaci a vzájemnou integraci, zejména provést:
   1.1. pořízení a implementaci Next Generation Firewall (NGFW),
   1.2. pořízení a implementaci Endpoint protection řešení (EDR),
   1.3. pořízení a implementaci nástroje pro analýzu a monitoring síťového provozu – nástroje pro ochranu integrity komunikačních sítí,
   1.4. pořízení serverů a diskových úložišť, switchů a ostatního HW,
   1.5. pořízení a implementaci nástroje pro zajišťování úrovně dostupnosti informací a efektivního zálohování,
   1.6. vybudování WiFi přístupového bodu,
   1.7. pořízení a implementaci nástroje pro multifaktorovou autentizaci a jednotné přihlašování,
   1.8. poskytnout Objednateli veškeré potřebné licence k dodanému řešení,
   1.9. provést zaškolení administrátorů a uživatelů na straně Objednatele,
   1.10. provést zkušební provoz a akceptační testy,
   1.11. zpracovat a předat Objednateli veškerou dokumentaci dodaného a implementovaného řešení do infrastruktury Objednatele,
   1.12. zajistit projektové vedení po celou dobu realizace plnění,
   1.13. poskytnout standardní záruku na dodané řešení,

   (dále společně jako „***předmět plnění***“).
2. Předmětem této Smlouvy je rovněž závazek Dodavatele:
   2.1. poskytnout Objednateli **nadstandardní (prodlouženou) záruku,** nepokrývá-li standardně poskytovaná záruka pro dodávané plnění či jeho část období 60-ti měsíců od převzetí předmětu plnění Objednatelem;

2.2. poskytnout Objednateli **technickou podporu (maintenance support + základní technická podpora)** dodaného a implementovaného řešení po dobu udržitelnosti projektu (min. 60 měsíců od převzetí předmětu plnění Objednatelem), a

2.3. poskytnout Objednateli **rozšířenou servisní podporu** dodaného a implementovaného řešení na základě písemných požadavků Objednatele po dobu udržitelnosti projektu (min. 60 měsíců od převzetí předmětu plnění Objednatelem).

3. Minimální technické, funkční a implementační/integrační požadavky na předmět plnění, a požadavky na poskytování dalších služeb, jak jsou vymezeny Objednatelem, a v rozsahu, v jakém se je zavázal naplňovat Dodavatel pro celou dobu plnění této Smlouvy, jsou závazně uvedeny v příloze č. 1 této Smlouvy.

4. Dodavatelem nabízený předmět plnění a zejména způsob jeho provedení musí splňovat požadavky stanovené vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

5. Dodavatel poskytne Objednateli předmět plnění na základě písemného projektu, který bude obsahovat zejména:

   5.1. popis dodávaného řešení (specifikaci dodávaného HW a SW, funkční schéma řešení),

   5.2. popis způsobu a postupu implementace do infrastruktury Objednatele,

   5.3. popis zabezpečení dodávaného řešení včetně zabezpečení informačních a komunikačních systémů v průběhu provádění díla),

   5.4. popis plánu zálohování a obnovy síťové infrastruktury,

   5.5. plán zkušebního provozu a provedení akceptačních testů,

   5.6. plán zaškolení administrátorů a uživatelů,

   5.7. harmonogram postupu prací v členění minimálně na kalendářní týdny,

   5.8. požadavky na součinnost Objednatele a období pro poskytnutí takové součinnosti, aj.

   (dále jen „***prováděcí projekt***“).

6. Dodavatel prohlašuje, že je oprávněn k distribuci programů a služeb, jež tvoří předmět této Smlouvy vymezený v předchozím odst. 1. tohoto článku Smlouvy, a touto Smlouvou poskytuje Objednateli oprávnění k jeho využívání v rozsahu a za podmínek v této Smlouvě vymezených.

7. Dodavatel se zavazuje, že využije ke zhotovení předmětu plnění pro Objednatele takové hardwarové či softwarové produkty a technologie, o kterých na základě své odbornosti a dostupných roadmap výrobců ví či může předpokládat, že budou schopny plnit účel vyplývající z této Smlouvy a budou výrobcem podporovány nejméně po dobu 60 měsíců od okamžiku dokončení předmětu plnění dle předpokladů stanovených touto Smlouvou a jejími přílohami. Tato skutečnost bude posuzována k datu podání nabídky Dodavatele, která předcházela uzavření této Smlouvy. Dodavatel splní tento závazek zejména tehdy, využije-li takové hardwarové či softwarové produkty a technologie, o nichž bylo v době podání nabídky před uzavřením této Smlouvy známo, že pro ně není vyhlášeno datum ukončení prodeje (end of sale), ani datum ukončení podpory/servisu (end od support/service). Nesplnění podmínky dle předchozí věty

se považuje za vadu plnění, pro kterou je Objednatel oprávněn plnění Dodavatele nepřevzít, a to až do okamžiku odstranění takové vady, zjistí-li tak před převzetím plnění; v ostatních případech bude Objednatel postupovat podle čl. XIII. odst. 3. této Smlouvy. Porušení uvedeného závazku a nezjednání nápravy dle této Smlouvy se považuje za podstatné porušení Smlouvy.

8. Předmětem této Smlouvy je závazek Objednatele zaplatit za Dodavatelem poskytnutý předmět plnění cenu sjednanou v čl. VI. této Smlouvy, v rozsahu Dodavatelem poskytnutého předmětu plnění dle přílohy č. 1 této Smlouvy a dle položkového ocenění podle přílohy č. 2 této Smlouvy.

IV. MÍSTO A DOBA PLNĚNÍ

1. Místem plnění je adresa sídla Objednatele:  Smluvní strany předpokládají poskytování předmětu plnění rovněž prostřednictvím dálkové komunikace a vzdáleného přístupu.

2. Dodavatel se zavazuje zahájit provádění předmětu plnění bezodkladně po nabytí účinnosti této smlouvy.

3. Smluvní strany se dohodly, že provádění předmětu plnění a jeho harmonogram bude respektovat jako nejzazší níže uvedené uzlové body (milníky):

Označení milníku	Název milníku	Trvání (nejpozději do)
T0	Zahájení plnění	po nabytí účinnosti Smlouvy
T1	Předložení prováděcího projektu Objednateli k akceptaci *(akceptační protokol/prohlášení)*	T0 + 4 kalendářní týdny
T2	Dodávka a implementace řešení – kyberbezpečnostní opatření *(akceptační protokol/prohlášení)*	T0 + 24 kalendářních týdnů
T3	Zpracování a předání dokumentace dodaného a implementovaného řešení; Školení administrátorů *(akceptační protokol/prohlášení)*	T0 + 26 kalendářních týdnů
T4	Zkušební provoz a akceptační testy *(akceptační protokol/prohlášení)*	T0 + 28 kalendářních týdnů
T5	Předání a převzetí dokončeného řešení a zahájení ostrého provozu *(protokol o předání a převzetí předmětu plnění)*	T0 + 28 kalendářních týdnů
T6	Poskytování technické podpory	T5 + 60 měsíců

4. Smluvní strany se dohodly, že podmínkou pro zahájení dodávky a implementace řešení do infrastruktury Objednatele (T2) je písemná akceptace prováděcího projektu Objednatelem. Objednatel se zavazuje provést posouzení prováděcího projektu dle čl. III. odst. 5. této Smlouvy a sdělit výsledek tohoto posouzení bez zbytečného odkladu po jeho předložení Dodavatelem, nejpozději však do 3 pracovních dnů od jeho předložení Dodavatelem. Za účelem dosažení akceptace prováděcího projektu Objednatelem ve lhůtě dle milníku T1 je Dodavatel oprávněn průběžně seznamovat Objednatele se stavem a obsahem tohoto prováděcího projektu. Objednatel je oprávněn vyzvat Dodavatele k poskytnutí rozpracované verze prováděcího projektu.

V případě, že prováděcí projekt nebude Dodavatelem zpracován v souladu s čl. III. odst. 5. této Smlouvy a/nebo bude vykazovat takové vady či nedostatky, v jejichž důsledku by bylo ohroženo naplnění účelu této Smlouvy vyjádřeného v čl. I. odst. 5. této Smlouvy, je Objednatel oprávněn odepřít akceptaci prováděcího projektu a sdělit důvody takového odepření akceptace. Nedojde-li k odstranění důvodů vedoucích k odepření akceptace prováděcího projektu ani v dodatečné lhůtě stanovené dohodou smluvních stran, je Objednatel oprávněn od této Smlouvy odstoupit. V případě akceptace prováděcího projektu Objednatelem v dodatečné lhůtě stanovené dohodou smluvních stran není dotčena odpovědnost Dodavatele za případné prodlení se splněním milníků dle předchozího odst. 3. tohoto článku Smlouvy. Odstoupí-li Objednatel od Smlouvy z důvodu uvedeného v tomto odstavci Smlouvy, nevzniká Dodavateli jakýkoliv nárok na úhradu ceny plnění či její části.

5. Smluvní strany se dohodly, že řádná a včasná dodávka a implementace řešení do infrastruktury Objednatele, včetně úspěšného absolvování zkušebního provozu, bude Dodavatelem předána Objednateli tak, aby Objednatel akceptoval a převzal dokončené řešení nejpozději **do 28 kalendářních týdnů ode dne nabytí účinnosti této Smlouvy**.

6. Smluvní strany se dohodly, že technická podpora bude Dodavatelem poskytována po dobu 60 měsíců ode dne akceptace a převzetí dokončeného řešení Objednatelem, není-li dále v této Smlouvě uvedeno jinak. Po uvedené období bude zajištěna platnost a trvání veškerých poskytnutých licencí.

V. PŘEDÁNÍ (ČÁSTI) PŘEDMĚTU PLNĚNÍ, AKCEPTACE

1. Smluvní strany se dohodly na tom, že Objednatel není povinen předmět plnění či jeho část převzít (akceptovat), pokud vykazuje vady či nedodělky, nenaplňuje veškeré požadavky, k jejichž splnění se Dodavatel zavázal, zejména pak požadavky plynoucí z přílohy č. 1 této Smlouvy anebo z prováděcího projektu, který Dodavatel předložil; zejména pak Objednateli náleží právo nepřevzít (neakceptovat) předmět plnění nebo jeho dílčí část v případě, kdy taková vada, nedodělek či rozpor s výše uvedenými dokumenty brání řádnému užívání předmětu plnění, resp. při návaznosti jednotlivých milníků dle čl. IV. odst. 3. této Smlouvy brání taková vada, nedodělek či rozpor v zahájení navazujícího milníku. Zároveň Objednatel není povinen předmět plnění převzít, pokud není proveden včas.

2. Akceptací předmětu plnění Objednatelem se závazek Dodavatele považuje za splněný, a výsledek plnění Dodavatele za způsobilý k užívání Objednatelem.

3. Akceptaci předmětu plnění Objednatelem bude předcházet ověření, zda plnění poskytnuté Dodavatelem dle této Smlouvy vedlo k výsledku a naplnění účelu, ke kterému se smluvní strany zavázaly, a to porovnáním skutečných vlastností jednotlivých částí plnění poskytnutých Dodavatelem dle této Smlouvy s jednotlivými požadavky pro ně stanovenými v této Smlouvě.

4. Předmět plnění se považuje za akceptovaný okamžikem podpisu příslušného protokolu ze strany Objednatele. Formálními náležitostmi protokolu o předání a převzetí předmětu plnění je jeho označení, datum vystavení, celkový počet stran, označení Smlouvy, označení Dodavatele a Objednatele, název projektu, označení a popis plnění, které je předmětem akceptace, datum zahájení a ukončení plnění, jméno a podpis osob, které protokol podepsaly. Protokol bude vyhotoven ve dvou výtiscích, přičemž každý bude určen pro jednu smluvní stranu. V protokolu bude zřetelně označeno, zda byl předmět plnění (i) akceptován, (ii) akceptován s výhradami, nebo (iii) neakceptován. Pokud bude předmět plnění

akceptován Objednatelem s výhradami, nebo nebude akceptován vůbec, bude k protokolu vyhotovena jeho příloha, ve které bude popis výhrad či vad, a bude zde zaznamenán také další dohodnutý postup a termíny odstranění těchto výhrad. Protokol bude podepsán oprávněnou osobou, která provedla na straně Objednatele akceptaci.

5. Před předáním předmětu plnění bude Dodavatel informovat Objednatele o termínu plánovaného předání plnění, a to písemně (alespoň prostřednictvím e-mailu) v dostatečném předstihu tak, aby vzhledem k charakteru předmětu plnění, jeho rozsahu a nárokům na kontrolu a ověření řádnosti a úplnosti jeho poskytnutí byly Objednateli vytvořeny podmínky k tomu, aby provedl kontrolu a ověření bez zbytečného odkladu po předání předmětu plnění Dodavatelem, a provedl akceptaci předmětu plnění ve lhůtě dle čl. IV. odst. 5 této Smlouvy.

6. V případě, že výsledek plnění Dodavatele neobsahuje dle Objednatele žádnou vadu či nedodělek a Objednatel nemá k plnění Dodavatele žádné výhrady ani připomínky, je předmět plnění akceptován bez výhrad, a tato skutečnost bude potvrzena v protokolu o předání a převzetí předmětu plnění.

7. V případě, že výsledek plnění Dodavatele obsahuje dle Objednatele drobné vady či nedodělky, které samostatně ani ve spojení s jinými nebrání užívání předmětu plnění k účelu stanovenému touto Smlouvou, nebo Objednatel má k výsledku plnění Dodavatele nepodstatné výhrady či připomínky, je předmět plnění akceptován s výhradami. Protokolu o předání a převzetí předmětu plnění tak bude obsahovat soupis vytknutých vad, nedodělků, výhrad či připomínek, a také způsoby a přiměřené lhůty pro jejich odstranění, na kterých se smluvní strany dohodly; nedohodnou-li se, budou odstraněny do 5-ti pracovních dnů. Smluvní strany považují v takovém případě výsledek plnění Dodavatele za Dodavatelem řádně předaný a Objednatelem řádně převzatý. Pakliže však nebudou Objednatelem vytknuté vady, nedodělky, výhrady či připomínky odstraněny v souladu se záznamem v protokolu a v termínech v něm uvedených, vzniká Objednateli nárok na smluvní pokutu dle sankčních ustanovení této Smlouvy. Dodavatel písemně informuje Objednatele o odstranění vad, nedodělků, výhrad či připomínek. Objednatel takto doplněný výsledek plnění bez zbytečného odkladu (nejpozději do 3 pracovních dnů od poskytnut informace Dodavatelem) posoudí, a odstranění vytknutých vad, nedodělků, výhrad či připomínek písemně potvrdí Dodavateli podepsáním přílohy protokolu.

8. V případě, že výsledek plnění Dodavatele trpí jinými než drobnými vadami či nedodělky, nebo Objednatel má k výsledku plnění Dodavatele podstatné výhrady či připomínky, pak předávaný předmět plnění neakceptuje. Smluvní strany nepovažují v takovém případě výsledek plnění Dodavatele za řádně předaný a Dodavatel je s předáním předmětu plnění v prodlení. Dodavatel je povinen bez zbytečného odkladu odstranit Objednatelem vytknuté vady, nedodělky, výhrady či připomínky, nebo poskytnout nové plnění. O této skutečnosti bude vyhotoven akceptační protokol, avšak v případě neakceptování předmětu plnění je Dodavatel po sjednání nápravy povinen znovu podstoupit celý proces akceptace podle této Smlouvy, aby mohl být předmět plnění Objednatelem akceptován. Tím není dotčena odpovědnost Dodavatele za prodlení s předáním předmětu plnění dle této Smlouvy, ani práva Objednatele z prodlení Dodavatele vyplývající z této Smlouvy.

9. Posouzení skutečnosti, zda vady či nedodělky zjištěné Objednatelem brání užívání předmětu plnění nebo jeho části, náleží výhradně Objednateli. Za vady či nedodělky je pro účely této Smlouvy považováno i dodání nesprávného druhu nebo množství částí předmětu plnění či nedodání jakýchkoliv dokladů či jiné dokumentace, které jsou k řádnému užívání předmětu plnění nezbytné.

10. Při předání předmětu plnění a podpisu protokolu si smluvní strany poskytnou vzájemnou součinnost. K účasti na akceptačním řízení a k podpisu protokolu o předání a převzetí předmětu plnění jsou vedle statutárních zástupců smluvních stran oprávněny tyto osoby:

    10.1. na straně Objednatele: [redacted]

    10.2. na straně Dodavatele: [redacted]

11. Den podpisu protokolu o předání a převzetí předmětu plnění je rozhodným dnem pro počátek běhu sjednané záruční doby a pro zahájení poskytování služeb technické podpory provozu dodaného řešení.

VI. CENA PLNĚNÍ A PLATEBNÍ PODMÍNKY

1. Ceny plnění dále uvedené v tomto článku Smlouvy jsou cenami úplnými v rozsahu stanoveném přílohou č. 2 této Smlouvy, a zahrnují veškeré náklady Dodavatele k poskytnutí předmětu plnění dle čl. III. odst. 1. a odst. 2. této Smlouvy. Celková cena plnění v uvedeném rozsahu činí:

    11.798.300,00 Kč bez DPH

    výše DPH 21 % 2 477 643 Kč

    14.275.943,00 Kč včetně DPH

    (slovy: čtrnáct milionů dvě stě sedmdesát pět tisíc devět set čtyřicet tři korun českých)

2. Celková cena plnění dle předchozího odstavce se sestává z cen za dílčí části plnění, a to ve výši:

    2.1. **Cena za dodávku a implementaci řešení v rozsahu čl. III. odst. 1. této smlouvy vč. standardní záruky** **10.656.000,00 Kč bez DPH,**

    2.2. **Cena za poskytnutí nadstandardní (prodloužené) záruky pro 4. a 5. rok plnění** **42.300,00 Kč bez DPH,**
    2.2.1. tj. roční plnění (12 měsíců) činí 21.150,00 Kč bez DPH,

    2.3. **Cena za poskytnutí potřebné maintenance support a Základní technické podpory na 5 let (1. až 60. měsíc)** **942.300,00 Kč bez DPH**,
    2.3.1. tj. roční plnění maintenance support (12 měsíců) činí 8.460,00 Kč bez DPH,
    2.3.2. tj. roční plnění základní tech. podpory (12 měsíců) činí 180.000,00 Kč bez DPH,

    2.4. **Cena za poskytnutí rozšířené servisní podpory na 5 let (předpokládaná kalkulace 100 hodin)** **200.000,00 Kč bez DPH,**
    2.4.1. tj. cena za 1 hodinu služeb rozšířené servisní podpory činí 2.000,00 Kč bez DPH,

3. Výše cen za jednotlivé položky plnění je uvedena v příloze č. 2 této Smlouvy. Za správnost stanovení sazby DPH a výše DPH odpovídá Dodavatel. Sazba DPH a výše DPH bude na faktuře Dodavatele stanovena vždy v aktuálně platné výši.

4. Cena plnění bude hrazena po částech, a to následovně:

   4.1. Cena dílčí části plnění dle čl. VI. odst. 2.1. této Smlouvy bude uhrazena **jednorázově**, a to po předání a převzetí plnění a podpisu protokolu dle čl. V. odst. 10. této Smlouvy Objednatelem. Datem uskutečnění zdanitelného plnění je den podpisu protokolu o předání a převzetí předmětu plnění Objednatelem.

   4.2. Cena dílčí části plnění dle čl. VI. odst. 2.2. této Smlouvy bude hrazena postupně **v pravidelných ročních paušálních platbách**, ve výši podílu připadajícího na roční plnění dle odst. 2.2.1. tohoto článku Smlouvy, a to pro každý nadcházející rok **předem**. Datem uskutečnění zdanitelného plnění je den zahájení poskytování nadstandardní (prodloužené) záruky dle této Smlouvy pro příslušný rok.

   4.3. Cena dílčí části plnění dle čl. VI. odst. 2.3. této Smlouvy bude hrazena postupně **v pravidelných ročních paušálních platbách**, ve výši podílu připadajícího na roční plnění dle odst. 2.3.1. a odst. 2.3.2. tohoto článku Smlouvy, a to pro každý nadcházející rok **předem**. Datem uskutečnění zdanitelného plnění je den výročí zahájení poskytování technické podpory dle této Smlouvy. Pro první rok poskytování technické podpory se za datum uskutečnění zdanitelného plnění považuje první den zahájení poskytování technické podpory následující po předání a převzetí předmětu plnění Objednatelem.

   4.4. Cena dílčí části plnění dle čl. VI. odst. 2.4. této Smlouvy bude hrazena postupně dle míry skutečné spotřeby časových jednotek (1 hodina = 60 minut) násobených hodinovou sazbou dle odst. 2.4.1. tohoto článku Smlouvy, při poskytování služeb rozšířené servisní podpory realizované Dodavatelem na základě písemně zadaných požadavků Objednatele, a to po konci kalendářního měsíce, ve kterém byly takové služby Objednatelem od Dodavatele čerpány. Datem uskutečnění zdanitelného plnění je poslední den příslušného kalendářního měsíce.

5. Dodavatel vystaví Objednateli daňový doklad (fakturu) na plnění v souladu s odst. 4. tohoto článku Smlouvy. Minimální doba splatnosti faktury vystavené ze strany Dodavatele bude činit 30 dní od doručení faktury Objednateli. Faktura bude splňovat náležitosti účetního dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a daňového dokladu podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.

6. Dodavatel je povinen vystavit a předat veškeré faktury v elektronickém formátu PDF, a zaslat je datovou zprávou do Datové schránky Objednatele – IDS: 8khyzqh.

7. Nezbytnou přílohou faktury bude zejména soupis skutečně dodaného plnění a provedených prací – zjišťovací protokol; v případě služeb rozšířené servisní podpory Objednatelem odsouhlasený soupis poskytnutých služeb s jejich časovým rozsahem. Přílohy budou připojeny v souboru ZIP nebo RAR v pořadí – 1. faktura jako hlavní dokument, 2. přílohy k faktuře jako příloha dokumentu. Plnění či práce, které provedl Dodavatel bez souhlasu Objednatele nad rámec předmětu této Smlouvy, nebudou do soupisu skutečně dodaného plnění a provedených prací zařazeny a považují se za součást celkové ceny, vyjma případů, kdy se smluvní strany písemně dohodnou jinak.

8. Faktura bude nad rámec zákonem požadovaných náležitostí (§ 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty) pro daňový doklad obsahovat také:

   a) číslo a datum vystavení faktury,

b) číslo smlouvy a datum jejího uzavření,
c) předmět plnění a jeho přesnou specifikaci ve slovním vyjádření,
d) soupis provedených prací včetně zjišťovacího protokolu
e) označení banky a číslo účtu, na který musí být zaplaceno (pokud je číslo účtu odlišné od čísla uvedeného v této Smlouvě, je Dodavatel povinen o této skutečnosti informovat Objednatele), číslo a datum příslušných akceptačních protokolů podepsaných zástupcem Dodavatele a odsouhlasených zástupcem Objednatele,
f) lhůtu splatnosti faktury,
g) název, sídlo, IČO a DIČ Objednatele a Dodavatele,
h) název a registrační číslo projektu: Zajištění kybernetické bezpečnosti VOŠZ Brno, příspěvková organizace, reg. č. projektu CZ.31.2.0/0.0/0.0/23_092/0008821,
i) jméno a podpis osoby Dodavatele, která fakturu vystavila, včetně kontaktního telefonu.

9. Nebude-li faktura obsahovat zákonem či touto Smlouvou stanovené náležitosti nebo bude chybně vyúčtována cena nebo DPH, je Objednatel oprávněn fakturu před uplynutím lhůty splatnosti vrátit Dodavateli k provedení opravy s vyznačením důvodu vrácení. Dodavatel provede opravu vystavením nové faktury. Dnem odeslání vadné faktury Objednatelem Dodavateli přestává běžet původní lhůta splatnosti a nová lhůta splatnosti počíná běžet znovu ode dne doručení nové a řádně vystavené faktury Objednateli.

10. V případě prodlení Objednatele se zaplacením řádně vystavené a doručené faktury se Objednatel zavazuje Dodavateli uhradit úrok z prodlení v zákonné výši.

11. Ceny plnění jsou uvedeny jako pevné a nejvýše přípustné ve vztahu k předmětu plnění v rozsahu stanoveném touto Smlouvou k okamžiku jejího uzavření, není-li v této Smlouvě výslovně uvedeno jinak. Smluvní strany sjednaly, že cena plnění zahrnuje rovněž náklady akceptačního řízení, zkušebního či testovacího provozu, technické podpory a servisu, a dalších služeb poskytovaných Dodavatelem Objednateli po dobu trvání této Smlouvy, a rovněž náklady na odstraňování vad a nedodělků plnění a vad plnění v průběhu záruky, včetně odměny za veškeré licence, které byly Objednateli poskytnuty na základě této Smlouvy, není-li dále ujednáno jinak. Dodavatel v souvislosti s ujednáním ceny předmětu plnění na sebe přebírá nebezpečí změny okolností ve smyslu § 2620 odst. 2 občanského zákoníku.

12. V případě, že dojde ke změně zákonné sazby DPH, je Dodavatel k ceně předmětu plnění bez DPH povinen účtovat DPH v platné výši. Tato situace představuje výjimku z nezměnitelnosti ceny předmětu plnění, přičemž smluvní strany výslovně uvádějí, že v případě změny ceny předmětu plnění v důsledku změny sazby DPH nebude ke Smlouvě uzavírán dodatek.

13. Smluvní strany si dále v souladu s § 100 odst. 1 ZZVZ, pro případ trvání a plnění této Smlouvy i po uplynutí prvních 60 měsíců poskytování technické podpory dle čl. III. odst. 2.2. a souvisejících této Smlouvy, vyhrazují právo stanovit pro 6. rok plnění a roky následující způsob stanovení ceny za poskytování technické podpory, a to dle dále uvedených pravidel:

    13.1. Výchozí hodnotou je vždy cena za poslední rok poskytování technické podpory (výchozí hodnotou pro stanovení ceny pro 6. rok plnění je tak cena za 5. rok plnění dle čl. VI. odst. 2.3.1. a odst. 2.3.2. této Smlouvy, resp. příslušné položky dle přílohy č. 2),

    13.2. Výchozí hodnota může být pro následující rok (12 měsíců) procentuálně zvýšena maximálně o míru inflace v ČR vyjádřenou přírůstkem průměrného ročního indexu spotřebitelských cen dle údajů publikovaných Českým statistickým úřadem za rok nejblíže předcházející. Ke stanovení

hodnoty plnění pro následující rok dojde na základě jednání a souhlasu obou smluvních stran, při respektování maximálního limitu nárůstu dle předchozí věty. Faktické zvýšení hodnoty za poskytování technické podpory bude projeveno ve faktuře vystavené v souladu s odst. 4.3. tohoto článku Smlouvy; uzavření písemného dodatku k této Smlouvě se pro tento případ nevyžaduje.

13.3. Smluvní strany jsou povinny si vzájemně oznámit svůj zájem na pokračování poskytování technické podpory pro každý následující rok plnění nejpozději 6 měsíců před uplynutím aktuálního roku poskytované technické podpory, nebo v téže lhůtě závazek k poskytování technické podpory pro následující rok vypovědět. V případě výpovědi kterékoliv smluvní strany dle předchozí věty zaniknou závazky smluvních stran k poslednímu dni období aktuálního roku poskytované technické podpory.

14. Smluvní strany si dále v souladu s § 100 odst. 1 ZZVZ, pro případ trvání a plnění této Smlouvy i po uplynutí prvních 60 měsíců poskytování rozšířené servisní podpory dle čl. III. odst. 2.3. a souvisejících této Smlouvy, vyhrazují právo stanovit pro 6. rok plnění a roky následující způsob stanovení ceny za poskytování rozšířené servisní podpory, a to dle dále uvedených pravidel:

14.1. Výchozí hodnotou je vždy cena za 1 hodinu (hodinová sazba) v posledním roce poskytování rozšířené servisní podpory (výchozí hodnotou pro stanovení hodinové sazby pro 6. rok plnění je tak hodinová sazba za 5. rok plnění dle čl. VI. odst. 2.4.1. této Smlouvy),

14.2. Výchozí hodnota může být pro následující rok (12 měsíců) procentuálně zvýšena maximálně o míru inflace v ČR vyjádřenou přírůstkem průměrného ročního indexu spotřebitelských cen dle údajů publikovaných Českým statistickým úřadem za rok nejblíže předcházející. Ke stanovení hodinové sazby pro následující rok dojde na základě jednání a souhlasu obou smluvních stran, při respektování maximálního limitu nárůstu dle předchozí věty. Faktické zvýšení hodinové sazby za poskytování rozšířené servisní podpory bude projeveno ve faktuře vystavené v souladu s odst. 4.4. tohoto článku Smlouvy; uzavření písemného dodatku k této Smlouvě se pro tento případ nevyžaduje.

VII. PRÁVA A POVINNOSTI DODAVATELE, PRAVIDLA VZDÁLENÉHO PŘÍSTUPU DODAVATELE

1. Dodavatel je povinen provést předmět plnění v rozsahu a termínech specifikovaných touto Smlouvou, jejími přílohami, a prováděcím projektem. Zjistí-li Dodavatel překážky, které znemožňují provést předmět plnění dohodnutým způsobem či ve stanovených termínech, je povinen to neprodleně písemně oznámit Objednateli a navrhnout mu změnu v řešení. Jakékoliv změny v řešení, které by vedly ke změně podmínek sjednaných touto Smlouvou, podléhají písemnému schválení Objednatele. Ustanovení § 222 ZZVZ tímto není dotčeno.

2. Dodavatel je povinen provést předmět plnění v souladu s obecně závaznými právními předpisy a v souladu se závaznými interními předpisy Objednatele.

3. Dodavatel je povinen provést předmět plnění řádně a odborně, sám nebo prostřednictvím svých poddodavatelů, které Dodavatel vůči Objednateli identifikuje.

4. Dodavatel není oprávněn postoupit třetí straně jakákoliv práva, nároky či pohledávky plynoucí z této Smlouvy bez předchozího písemného souhlasu Objednatele.

5. Pokud bude při provádění předmětu plnění Dodavatelem využito i volně šiřitelné programové vybavení, je Dodavatel povinen zpracovat přehled licencí a předložit ho jako součást akceptačního protokolu. Dodavatel je povinen zajistit, že poskytnutím uvedených licencí nedojde k porušení práv třetích stran.

6. Dodavatel je povinen určit kontaktní osobu řídící evidenci osob Dodavatele oprávněných k přístupu do síťové infrastruktury Objednatele. V případě změny této kontaktní osoby je Dodavatel povinen bezodkladně oznámit Objednateli takovou změnu, včetně sdělení nové kontaktní osoby.

7. Přístup k síťové infrastruktuře Objednatele je možné povolit pouze po předchozím provedení evidence osoby zastupující Dodavatele v registru identit Objednatele nebo obdobném systému Objednatele, a to na základě požadavku Dodavatele na přístup. Přidělení oprávnění zaměstnancům Dodavatele bude řízeno principem nezbytného minima a není nárokové. Systém pro přístup do síťové infrastruktury Objednatele určí Objednatel.

8. Dodavatel se zavazuje, že neumožní, aby byl tentýž udělený přístup do síťové infrastruktury Objednatele sdílen více zaměstnanci Dodavatele, případně jeho poddodavateli či zaměstnanci poddodavatele.

9. Dodavatel se zavazuje zajistit, aby osoby podílející se na poskytování předmětu plnění této Smlouvy Objednateli, které přistupují do interní sítě, chránily autentizační prostředky a údaje. Dodavatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako kybernetická bezpečnostní událost ve smyslu příslušné řídící dokumentace, a mohou být uplatněny příslušné postupy zvládání kybernetické bezpečnostní události (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu). Dodavatel bere na vědomí, že postup zvládáním kybernetické bezpečnostní události či jiný důsledek porušení bezpečnostních opatření nebude posuzován jako okolnost vylučující odpovědnost Dodavatele za prodlení s řádným a včasným plněním předmětu této Smlouvy, a nebude důvodem k jakékoli náhradě případné újmy způsobené Dodavateli či jiné osobě na jeho straně.

10. Dodavatel se zavazuje, že neumožní připojit koncové zařízení do sítě Objednatele bez předchozího schválení připojení určenou osobu na straně Objednatele.

11. Dodavatel se zavazuje, že všechny jeho informační systémy, které se budou připojovat do síťové infrastruktury Objednatele, jsou a budou chráněny vhodným způsobem proti malware.

12. Dodavatel je povinen mít po celou dobu trvání této Smlouvy zajištěno **pojištění odpovědnosti za škodu** způsobenou třetí osobě, přičemž pojistná částka musí svou výší odpovídat minimálně 10.000.000 Kč. Dodavatel je povinen pojistnou smlouvu, nebo potvrzení o pojištění, předložit Objednateli bezodkladně po uzavření této Smlouvy, nejpozději však do předložení prováděcího projektu před zahájením dodávky a implementace řešení, a dále pak v průběhu provádění předmětu plnění kdykoliv na vyzvání Objednatele.

13. Dodavatel se zavazuje při provádění předmětu plnění dle této Smlouvy zajistit dodržování veškerých pracovněprávních předpisů (odměňování, pracovní doba, doba odpočinku mezi směnami, placené přesčasy, legální zaměstnávání pracovníků), dále předpisů týkajících se oblasti zaměstnanosti a bezpečnosti a ochrany zdraví při práci, tj. zejména zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, a to vůči všem osobám, které se na plnění předmětu této smlouvy podílejí, bez ohledu na to, zda budou činnosti prováděné v rámci plnění předmětu této Smlouvy prováděny přímo Dodavatelem a jeho zaměstnanci, či poddodavatelem. Dodavatel se zavazuje, že provádění předmětu plnění dle této Smlouvy bude prováděno v souladu s úmluvami Mezinárodní organizace práce, jimiž je Česká republika vázána, zejména s

úmluvami, které upravují stejné odměňování pracujících mužů a žen za práci stejné hodnoty, diskriminaci, bezpečnost a zdraví pracovníků, a pracovní prostředí.

14. Dodavatel se zavazuje zachovávat férové vztahy ke svým poddodavatelům. Jakýkoliv závazek uzavřený mezi Dodavatelem a jeho poddodavatelem v souvislosti s plněním (části) předmětu této smlouvy nesmí obsahovat splatnost faktury delší než 30 dnů.

15. Dodavatel se zavazuje při realizaci předmětu této Smlouvy k šetrnému využívání zdrojů a materiálů, k řádnému managementu nakládání s odpady a k omezení jejich nadbytečné produkce.

16. Objednatel je oprávněn průběžně kontrolovat dodržování povinností dodavatele dle odst. 13. až 15. tohoto článku Smlouvy, přičemž Dodavatel je povinen tuto kontrolu umožnit, strpět a poskytnout Objednateli veškerou nezbytnou součinnost k jejímu provedení. Zjistí-li Objednatel, že Dodavatel porušil některou z povinností dle odst. 13. až 15. tohoto článku Smlouvy, a nesjednal nápravu ani po předchozím písemném upozornění Objednatele, je Objednatel oprávněn od této smlouvy odstoupit pro podstatné porušení povinnosti Dodavatele.

VIII.PRÁVA A POVINNOSTI OBJEDNATELE

1. Objednatel se zavazuje poskytnout Dodavateli součinnost, která je nezbytná k řádnému poskytnutí předmětu plnění této Smlouvy, a lze ji po něm spravedlivě požadovat.

2. Objednatel je oprávněn průběžně vykonávat kontrolu provádění předmětu plnění. Dodavatel umožní provádění kontroly kdykoli během provádění předmětu plnění všem oprávněným osobám určeným Objednatelem. Dodavatel se též zavazuje předkládat Objednateli na jeho žádost ústní či písemné informace o průběhu a obsahu prováděného plnění, a to nejpozději do 2 (dvou) pracovních dnů od doručení žádosti Objednatele. Pro kontrolu provádění plnění platí:

   a) Objednatel alespoň 2 (dva) pracovní dny přede dnem plánované kontroly dle přechozího odstavce písemně sdělí Dodavateli termín kontroly. Dodavatel zajistí přítomnost osoby odpovědné za provádění příslušné části předmětu plnění po celou dobu konání kontroly.

   b) O výsledku kontroly smluvní strany provedou písemný zápis ve 2 (dvou) vyhotoveních, každá ze smluvních stran obdrží po 1 (jednom) vyhotovení zápisu.

   c) Objednatel je oprávněn na základě provedené kontroly požadovat, aby Dodavatel provedl nápravu zjištěného porušení povinnosti Dodavatele nebo odstranění zjištěné vady, a aby plnění poskytoval řádným způsobem.

   d) Dodavatel za účelem vykonání kontroly poskytne osobě pověřené Objednatelem výkonem kontroly veškerou nezbytnou součinnost potřebnou pro řádné plnění jejích povinností.

3. Objednatel se zavazuje uhradit Dodavateli řádně a včas veškeré finanční závazky vyplývající z této Smlouvy.

IX. TRVÁNÍ SMLOUVY A UKONČENÍ SMLOUVY

1. Smluvní strany se dohodly, že tato Smlouva se sjednává na dobu od okamžiku účinného uzavření této Smlouvy do ukončení technické podpory poskytnutého předmětu plnění.

2. Smluvní strany sjednávají poskytování technické podpory předmětu plnění na dobu neurčitou, nebo do doby jejího dřívějšího ukončení podle předchozích ustanovení této Smlouvy nebo podle následujících odstavců tohoto článku Smlouvy.

3. Smluvní strany sjednávají možnost předčasného ukončení této Smlouvy písemnou dohodou smluvních stran.

4. Smluvní strany se dohodly, že mohou od této Smlouvy odstoupit v případech, kdy to stanoví zákon nebo tato Smlouva. Odstoupení od Smlouvy musí být provedeno písemnou formou a je účinné okamžikem jeho doručení druhé smluvní straně. Odstoupením od Smlouvy nezanikají nároky na náhradu škody, smluvní ujednání týkající se volby práva, smluvních pokut, řešení sporů mezi smluvními stranami a jiná ujednání, která podle projevené vůle smluvních stran nebo vzhledem ke své povaze mají trvat i po ukončení Smlouvy. Zejména se jedná o práva a povinnosti související s odpovědností za škodu, smluvními pokutami, fakturací cen, s úroky z prodlení, odpovědností za vady, ochranou osobních údajů a důvěrných informací apod.

5. Objednatel je oprávněn odstoupit od této Smlouvy zejména, nikoli však výlučně, v případě, kdy:

   a) prodlení Dodavatele s předáním předmětu plnění k termínu stanoveném čl. IV. odst. 5. této Smlouvy trvá déle než 15 kalendářních dnů;

   b) prodlení Dodavatele se splněním povinnosti odstranit vady či nedodělky uvedené v protokolu o předání a převzetí předmětu plnění trvá déle než 7 kalendářních dnů od smluvními stranami sjednaného či Smlouvou stanoveného termínu;

   c) z průběžně prováděné kontroly vyvstanou důvodné pochybnosti o schopnosti Dodavatele splnit předmět plnění řádně a úplně, a Dodavatel nebude schopen na výzvu Objednatele tyto objektivní důvody vyvrátit;

   d) předmět plnění vykazuje vady či nedodělky, které neumožní jeho řádné užívání k účelu, který je sjednán touto Smlouvou,

   e) prokáže-li se kterékoliv prohlášení Dodavatele učiněné v této Smlouvě jako nepravdivé,

   f) Dodavatel neplní pokyny Objednatele při poskytování předmětu plnění, a nezjedná nápravu do 7 kalendářních dnů poté, co byl Objednatelem na tuto skutečnost písemně upozorněn,

   g) Dodavatel brání Objednateli v provádění kontrol či zkoušek předmětu plnění nebo jeho částí, či více než 7 kalendářních dnů neposkytuje součinnost, ke které se zavázal touto Smlouvou,

   h) pokud Dodavatel nevyhoví požadavku Objednatele na výměnu poddodavatele, pokud byly splněny podmínky podle této Smlouvy,

   i) poruší-li Dodavatel opakovaně (více než dvakrát) pravidla pro vzdálený přístup Dodavatele stanovená v čl. VII. této Smlouvy nebo nezajistí-li jejich dodržování,

   j) v případech vymezených § 223 odst. 1 až 3 ZZVZ,

   k) dostane-li se Dodavatel do stavu úpadku nebo hrozícího úpadku, dojde-li k zahájení likvidace Dodavatel, nebo dojde-li k postižení podstatné části majetku Dodavatel výkonem rozhodnutí nebo exekucí.

6. Dodavatel je oprávněn odstoupit od této Smlouvy v případě prodlení Objednatele se zaplacením jakékoliv splatné částky dle této Smlouvy po dobu delší než 60 kalendářních dnů, pokud Objednatel nezjedná

nápravu ani v dodatečné přiměřené lhůtě, kterou mu k tomu Dodavatel poskytne v písemné výzvě ke splnění povinnosti, přičemž tato lhůta nesmí být kratší než 15 kalendářních dnů od prokazatelného doručení takovéto výzvy Objednateli. Toto ustanovení se dle dohody smluvních stran nevztahuje na případy, kdy bude prodlení Objednatele zapříčiněno opožděným uvolněním finančních prostředků z veřejných zdrojů.

7. V případě odstoupení od Smlouvy nemá Dodavatel nárok na zaplacení ceny předmětu plnění v plném rozsahu. Dodavatel je pouze oprávněn žádat po Objednateli to, o co se Objednatel poskytnutím předmětu plnění Dodavatelem obohatil, a to v rozsahu plnění, které je Objednatelem využitelné i po takovém odstoupení od Smlouvy.

8. Smluvní strany se dohodly, že v případě předčasného ukončení Smlouvy odstoupením od Smlouvy si poskytnou vzájemnou součinnost k převodu a nabytí licencí či oprávnění plynoucích z takových licencí již pořízených Dodavatelem pro Objednatele, kterými Objednatel nedisponuje, resp., které Objednatel případně dosud neuhradil Dodavateli podle čl. VI. této Smlouvy. Dodavatel je povinen takové licence převést na Objednatele, a Objednatel je povinen je nabýt a uhradit za ně Dodavateli cenu stanovenou podle této Smlouvy, celkově nejvýše však do částky odpovídající výši platby za 1 rok, nebrání-li takovému převodu objektivní překážky ležící vně vůle smluvních stran.

9. Při předčasném ukončení závazku z této Smlouvy se Dodavatel zavazuje provést na své náklady veškeré práce, které budou nezbytné k zabránění vzniku škody či jiné újmy na straně Objednatele či na straně třetích osob. Dodavatel bude v takovém případě rovněž povinen předat Objednateli bezplatně veškeré informace, které s dílem souvisí a jsou nezbytné k zabránění vzniku škody či jiné újmy na straně Objednatele či třetích osob.

X. REALIZAČNÍ TÝM

1. Dodavatel provede předmět plnění zejména prostřednictvím osob, které jsou uvedeny v příloze č. 3 této Smlouvy. Jedná se o osoby, kterými Dodavatel prokazoval splnění části technické kvalifikace v rámci své účasti v zadávacím řízení veřejné zakázky.

2. Dodavatel prohlašuje, že se všichni členové realizačního týmu, jimiž v rámci zadávacího řízení veřejné zakázky prokazoval splnění kvalifikace, budou aktivně podílet na provedení příslušné části předmětu plnění podle této Smlouvy a nabídky podané v rámci zadávacího řízení veřejné zakázky.

3. V případě, že kvalita předmětu plnění dle této Smlouvy prováděná některým z členů realizačního týmu neodpovídá požadavkům této Smlouvy, nebo člen realizačního týmu nevykonává pokyny Objednatele podle Smlouvy, nebo nastane jiný závažný důvod pro změnu realizačního týmu, pak je Objednatel oprávněn požadovat výměnu člena realizačního týmu. Dodavatel do 10 kalendářních dnů od doručení žádosti Objednatele navrhne nového člena realizačního týmu, přičemž nově navržený člen realizačního týmu musí disponovat stejnou nebo vyšší úrovní kvalifikace, jakou disponoval původní člen realizačního týmu, kterým byla prokazována kvalifikace v rámci zadávacího řízení veřejné zakázky, resp. v případě v zadávacím řízení veřejné zakázky hodnoceného člena realizační týmu stejnou nebo vyšší hodnocenou kvalitativní úrovní. Nový člen realizačního týmu následně musí být akceptován ze strany Objednatele. Akceptace nového člena realizačního týmu je podmíněna předložením dokladů, prokazujících dosažení minimálně shodné úrovně jeho zkušeností jako u původního člena.

4. Pokud jsou důvody pro změnu některého ze členů realizačního týmu dány na straně Dodavatele, Dodavatel může ke změně přistoupit pouze ze závažných důvodů s předchozím souhlasem Objednatele. Nově navržený člen realizačního týmu přitom musí disponovat stejnou nebo vyšší úrovní kvalifikace, jakou disponoval člen realizačního týmu, kterým byla prokazována kvalifikace v rámci zadávacího řízení veřejné zakázky, resp. v případě v zadávacím řízení veřejné zakázky hodnoceného člena realizační týmu stejnou nebo vyšší hodnocenou kvalitativní úrovní Objednatel udělí písemný souhlas se změnou do 10 kalendářních dnů od doručení žádosti ze strany Dodavatele, jejíž přílohou budou doklady prokazující dosažení minimálně shodné úrovně zkušeností nového člena jako u původního člena.

5. Realizační tým Dodavatele může být tvořen i dalšími osobami nad rámec počtu stanoveného minimálními požadavky kvalifikace. Dodavatel se zavazuje, že při běžné pracovní komunikaci s Objednatelem či jeho zástupci bude užíváno českého nebo slovenského jazyka, nedohodnou-li se smluvní strany či jejich jednotlivý zástupci jinak.

XI. PODDODAVATELÉ

1. Dodavatel je oprávněn využít k provedení předmětu plnění jiné osoby pouze v případě, že tyto osoby jsou součástí seznamu poddodavatelů, který tvoří přílohu č. 4 této Smlouvy a který byl rovněž součástí nabídky Dodavatele do veřejné zakázky, není-li stanoveno jinak. Dodavatel se zavazuje, že poddodavatelé, kterými prokazoval splnění kvalifikace v zadávacím řízení veřejné zakázky, se budou podílet na plnění povinností Dodavatele vyplývajících ze Smlouvy v rozsahu podle nabídky Dodavatele podané do zadávacího řízení veřejné zakázky.

2. Dodavatel odpovídá za plnění poddodavatele tak, jako by plnil sám. Dodavatel je povinen vybrat takového poddodavatele, který neodporuje požadavkům, jaké má Objednatel na Dodavatele.

3. Dodavatel prohlašuje a zavazuje se, že ručí za uspokojení povinnosti poddodavatele nahradit újmu způsobenou poddodavatelem Objednateli při plnění nebo v souvislosti s plněním povinností ze Smlouvy, jestliže povinnost k náhradě újmy nesplnil poddodavatel sám.

4. V případě, že poddodavatel je s plněním svých závazků, které přímo souvisí s předmětem této smlouvy, v prodlení více než 10 kalendářních dnů, nebo byl poddodavateli uložen zákaz plnění veřejných zakázek, ocitnul se v úpadku nebo hrozícím úpadku, nebo byl pravomocně odsouzen za trestný čin uvedený v příloze č. 3 ZZVZ, nebo je zde jiný vážný důvod, pak je Objednatel oprávněn požadovat po Dodavateli výměnu poddodavatele. Za jiný vážný důvod dle předchozí věty se považuje rovněž stav nereflektování výhrad sdělených Objednatelem k činnosti poddodavatele, či řádnosti a kvality jím poskytovaného plnění apod., kdy uvedené nedostatky nebyly napraveny ani po předchozí písemné stížnosti adresované Objednatelem Dodavateli. Dodavatel je povinen navrhnout nového poddodavatele do 10 kalendářních dnů od doručení žádosti Objednatele. Nový poddodavatel se může podílet na poskytování předmětu plnění pouze na základě písemného souhlasu Objednatele, který Objednatel udělí po provedení kontroly dokladů předložených Dodavatelem k novému poddodavateli.

5. Pokud jsou důvody pro změnu či doplnění poddodavatele dány na straně Dodavatele, Dodavatel může ke změně či doplnění přistoupit pouze s předchozím souhlasem Objednatele. Jedná-li se o změnu poddodavatele, prostřednictvím něhož byla prokazována kvalifikace, nově navržený poddodavatel musí disponovat stejnou nebo vyšší úrovní kvalifikace, jakou disponoval poddodavatel, kterým byla prokazována kvalifikace v rámci zadávacího řízení veřejné zakázky. Objednatel udělí písemný souhlas se změnou

poddodavatele po doručení žádosti ze strany Dodavatele, jejíž přílohou budou doklady prokazující kvalifikaci nového poddodavatele, a po provedení kontroly takto předložených dokladů.

XII. VLASTNICKÉ PRÁVO A UŽÍVACÍ PRÁVA, DUŠEVNÍ VLASTNICTVÍ

1. Objednatel nabývá vlastnické právo k poskytnutému předmětu plnění podpisem akceptačního protokolu, a to v rozsahu akceptace.

2. Dodavatel se zavazuje při poskytování předmětu plnění neporušit práva třetích osob, která těmto osobám mohou plynout z duševního vlastnictví, zejména z autorských práv a práv průmyslového vlastnictví. Dodavatel se zavazuje, že Objednateli uhradí veškeré náklady, výdaje, škody a majetkovou i nemajetkovou újmu, které Objednateli vzniknou v důsledku uplatnění práv třetích osob vůči Objednateli v souvislosti s porušením povinnosti Dodavatele dle předchozí věty. Uplatní-li třetí osoba své právo k předmětu plnění nebo jeho části, zavazuje se Dodavatel dále Objednateli bezplatně poskytnout, zabezpečit a/nebo uhradit náhradní řešení, které nebude dotčeno právem třetí osoby.

3. V případě, že je výsledkem činnosti Dodavatele dle této Smlouvy či jeho součástí dílo, které podléhá ochraně podle zákona č. 121/2000 Sb., o právu autorském, právech souvisejících s právem autorským a o změně dalších zákonů (autorský zákon), v platném znění (dále jen „autorský zákon“) a občanského zákoníku, získá Objednatel k takto vytvořenému dílu jako celku i k jeho jednotlivým částem licenci, přičemž odměna za poskytnutou licenci je již součástí ceny předmětu plnění.

4. Pro účely této Smlouvy rozlišují smluvní strany mezi „Individualizovaným dílem“ a „Standardizovaným dílem“, kdy:

   - Individualizovaným dílem se rozumí dílo dodávané Dodavatelem dle této Smlouvy, které bylo vytvořeno nebo upraveno pro účely této Smlouvy;
   - Standardizovaným dílem se rozumí dílo dodávané Dodavatelem dle této Smlouvy, které nebylo vytvořeno nebo upraveno pro účely této Smlouvy.

   V případě pochybností se na plnění hledí jako na Individualizované dílo, dokud Dodavatel neprokáže opak.

5. Dodavatel na základě této Smlouvy poskytuje Objednateli oprávnění k výkonu práv duševního vlastnictví k Individualizovanému dílu. Licence se týká veškerých autorských nebo jiných duševních práv k Individualizovanému dílu, jejichž povaha umožňuje licenci v dále uvedeném rozsahu poskytnout, a to:

   a) licence k veškerým známým způsobům užití takového díla, zejména, nikoliv však výlučně, k účelu stanovenému touto Smlouvou a v rozsahu minimálně nezbytném pro řádné užívání příslušného Individualizovaného díla Objednatelem v souladu s touto Smlouvou;
   b) licence neodvolatelná a nevypověditelná;
   c) licence neomezená územním rozsahem a rovněž tak neomezená způsobem nebo rozsahem užití;
   d) licence udělená na dobu určitou, a to po celou dobu trvání majetkových práv k dílu (účinnost licence však trvá i po skončení účinnosti této Smlouvy, nedohodnou-li se Smluvní strany výslovně jinak);
   e) licence vztahující se i na budoucí aktualizace dodaného předmětu plnění v rámci jeho podpory;

f) licence převoditelná a postupitelná, tj. která je udělena s právem udělení podlicence či postoupení licence jakékoliv třetí osobě;
g) licence, kterou není Objednatel povinen využít.

6. Licence je poskytnutá v maximálním rozsahu povoleném platnými právními předpisy. Dodavatel podpisem Smlouvy prohlašuje, že vlastní či oprávněně disponuje veškerými oprávněními k autorskému dílu, které bude součástí předmětu plnění dle této Smlouvy, zejména, nikoliv však výlučně, že získal veškerá oprávnění autorů či třetích osob k takovému dílu a je oprávněn je poskytnout Objednateli, a to zejména, nikoliv však výlučně, veškerá oprávnění uvedená v tomto článku Smlouvy.

7. Dodavatel uděluje Objednateli souhlas k tomu, aby Objednatel (či jím pověřená třetí osoba) dle své potřeby zasahoval do Individualizovaného díla, zejm. je oprávněn jej zveřejnit, upravovat, zpracovávat, překládat, měnit jeho název, spojit s dílem jiným a zařadit jej do díla souborného. Ustanovení tohoto odstavce neomezuje práva Objednatele plynoucí z § 66 zákona č. 121/2000 Sb., autorský zákon.

8. Dodavatel se zavazuje zajistit oprávnění k užití předmětu práv duševního vlastnictví jiných osob, který představuje Individualizované dílo, a souhlas se zásahy do takového předmětu práv duševního vlastnictví v takovém rozsahu, aby Objednateli mohl udělit licenci k Individualizovanému dílu v rozsahu této Smlouvy, souhlas k zásahům ve smyslu předchozího odst. 7. tohoto článku Smlouvy, a aby mohl Objednateli předat zdrojový kód a dokumentaci k takovému předmětu práv duševního vlastnictví.

9. Jedná-li se o oprávnění k výkonu práv duševního vlastnictví ke Standardizovanému dílu, je Dodavatel povinen Objednateli poskytnout:

   a) licenci ke Standardizovanému dílu, pokud je autorem Standardizovaného díla Dodavatel, nebo
   b) zajistit poskytnutí licence ke Standardizovanému dílu Objednateli třetí osobou, pokud je autorem Standardizovaného díla jiná třetí osoba,

   a to v rozsahu, který zajistí plnou využitelnost Standardizovaného díla při jeho vývoji, rozvoji, provozu a užívání bez nutnosti platit Dodavateli nebo třetí osobě odměnu nad rámec odměny dle této Smlouvy. Nabyvatelem licence ke Standardizovanému dílu podle tohoto odstavce musí být bezprostředně Objednatel.

10. Dodavatel je při plnění této Smlouvy oprávněn použít tzv. free and open-source software (dále jen „FOSS“) s tím, že užití FOSS a licence se k tomu vztahující nesmí být v rozporu s účelem této Smlouvy. Dodavatel společně s předáním svého výstupu, který obsahuje FOSS, sdělí Objednateli informace o tom, že byl FOSS použit a jaké licenční podmínky se na užití FOSS vztahují. Využije-li Dodavatel při plnění této Smlouvy FOSS, zavazuje se zajistit po dobu trvání Smlouvy jeho podporu tak, aby nedošlo k omezení jeho funkčnosti či bezpečnosti, zejména v situaci, kdy původní tvůrce příslušného FOSS ukončí poskytování podpory. Odměna za jakékoliv plnění Dodavatele související se zajištěním podpory FOSS dle předchozí věty, včetně případného nahrazení FOSS bez podpory jiným software, je zahrnuta v odměně za poskytování technické podpory dle čl. VI. této Smlouvy a Dodavateli nenáleží žádná další odměna či kompenzace.

11. Dodavatel je povinen současně s předáním předmětu plnění, resp. těch částí předmětu plnění, které jsou počítačovým programem, předat Objednateli zdrojový kód včetně administrátorského přístupu k němu (dále jen „zdrojový kód“); výjimku z této povinnosti tvoří odst. 14. tohoto článku Smlouvy.

12. Zdrojový kód musí být spustitelný v prostředí Objednatele a zaručující možnost ověření, že je kompletní a ve správné verzi, tzn. umožňující instalaci, spuštění a ověření funkcionality, a to včetně podrobné

dokumentace zdrojového kódu, na základě které bude Objednatel schopen zjistit veškeré funkce a vnitřní vazby počítačového programu a zasahovat do něj. Zdrojový kód bude Objednateli Dodavatelem předán na nepřepisovatelném technickém nosiči dat s viditelně označeným názvem „Zdrojový kód“ a označením jeho verze a dne předání zdrojového kódu, případně na základě dohody smluvních stran bude k předání využito sdíleného elektronického úložiště, které zřídí Dodavatel a poskytne do něj Objednateli přístup. O předání zdrojového kódu bude smluvními stranami sepsán písemný protokol.

13. Povinnost Dodavatele uvedená v předcházejícím odstavci se přiměřeně použije i pro jakékoliv opravy, změny, doplnění, upgrade nebo update zdrojového kódu, k nimž dojde při provádění předmětu plnění nebo v rámci jeho oprav (dále jen „změna zdrojového kódu“). Dokumentace změny zdrojového kódu musí obsahovat podrobný popis a komentář každého zásahu do zdrojového kódu.

14. Výjimkou z ujednání týkajících se předání zdrojového kódu je situace, kdy součástí plnění je Standardizované dílo a předání zdrojového kódu ke Standardizovanému dílu není možné s ohledem na práva třetích osob.

15. Práva získaná v rámci plnění poskytnutého podle tohoto článku Smlouvy přechází i na případného právního nástupce Objednatele. Případná změna v osobě Dodavatele (např. právní nástupnictví) nebude mít vliv na oprávnění udělená v rámci této Smlouvy Dodavatelem Objednateli.

XIII. ODPOVĚDNOST ZA VADY, ZÁRUKA A TECHNICKÁ PODPORA

1. Dodavatel poskytuje záruku za dodané řešení v délce, která je pro jednotlivé součásti řešení uvedena v příloze č. 1 této Smlouvy, minimálně však standardní záruku po dobu prvních 36 měsíců od převzetí dokončeného řešení Objednatelem, a na ni v takovém případě navazující nadstandardní (prodlouženou) záruku v délce 24 měsíců následujících po uplynutí standardní záruky (nepokrývá-li standardně poskytovaná záruka pro dodávané plnění či jeho část delší než uvedené období či celé období 60-ti měsíců od převzetí předmětu plnění Objednatelem), celkem tedy 60 měsíců.

2. Dodavatel odpovídá za vady, které má předmět plnění v době jeho převzetí a akceptace, a za vady, které se projeví v záruční době, popřípadě v důsledku škody, za kterou odpovídá Dodavatel.

3. Veškeré vady předmětu plnění je Objednatel oprávněn uplatnit u Dodavatele kdykoliv po zjištění vady během záruky, a to formou písemného oznámení, obsahujícího specifikaci zjištěné vady nebo popis, jak se vada projevuje. Objednatel je oprávněn uplatnit veškerá zákonná práva z vadného plnění. Volba práva z vadného plnění svědčí Objednateli. Neuvede-li Objednatel, jaké právo v souvislosti s vadou předmětu plnění uplatňuje, má se za to, že požaduje odstranění vady, tj. provedení opravy předmětu plnění nebo jeho části.

4. Dodavatel v rámci předmětu plnění této Smlouvy poskytuje Objednateli rovněž technickou podporu a rozšířenou servisní podporu dodaného řešení. Toto plnění zahrnuje zejména (nikoli výlučně):

   - odstraňování nebo spolupráci při odstraňování závad či nefunkčností,
   - kontrolu stavu jednotlivých komponent řešení a po vzájemné dohodě aplikaci nápravných opatření,
   - řešení vzniknuvších problémů a incidentů,
   - bezplatná výměna vadného zařízení/komponentu,
   - aktualizace firmware a software dodaných produktů,

- aktualizaci dokumentace,
- na vyžádání změnu nastavení, konfiguraci řešení,
- podporu při implementaci upgradů,
- poskytování informací,
- poskytování odborných konzultací a podpory.

5. Za účelem poskytování služeb technické podpory, rozšířené servisní podpory a příjmu požadavků/hlášení incidentů Objednatele je Dodavatel povinen zřídit a udržovat po celou dobu trvání této Smlouvy systém HelpDesk. Systém HelpDesk bude dostupný na adrese: **servishw@aricoma.com**.

6. Příjem požadavků v systému HelpDesk musí být zajištěn v režimu 7x24. Samotná technická podpora Dodavatele bude poskytována min. v pracovní dny v pracovní době od 07:00 do 16:00 hodin (dále jen „*pracovní doba*“).

7. Dodavatel garantuje Objednateli čas pro odezvu a čas pro vyřešení provozního incidentu, a to pro jednotlivé kategorie provozních incidentů následovně:

Kategorie incident	Lhůta odezvy (IRT)	Lhůta vyřešení (TRT)
Kritický	1 hodina	12 hodin
Závažný	1 hodina	2 dny
Běžný	1 den	7 dní
Minoritní	3 dny	Best effort

8. Dodavatel je povinen vyřešit požadavek za podmínek stanovených v příloze č. 1 této Smlouvy ve lhůtě dohodnuté zástupci Objednatele a Dodavatele, a nedohodnou-li se, pak ve lhůtách stanovených v předchozím odst. 7 tohoto článku Smlouvy v souladu s přílohou č. 1 této Smlouvy.

9. Technická podpora bude Dodavatelem poskytována jak proaktivně (např. průběžné kontroly stavu komponent Dodavatelem), tak reaktivně (činnost Dodavatele vyvolaná na základě žádosti Objednatele). Kontaktními osobami v záležitostech poskytování technické podpory jsou:

   9.1. na straně Objednatele: 

   9.2. na straně Dodavatele: 

10. Dodavatel je povinen vést evidenci poskytování technické podpory a předkládat ji Objednateli pravidelně 1 x za čtvrtletí, nebo na žádost Objednatele mimo uvedený interval (dále jen „***reporty***“). Z reportů bude zřejmé, v jakém rozsahu a v jaké oblasti byly služby technické podpory poskytnuty, a jaká je bilance čerpání hodin základní technické podpory a rozšířené servisní podpory. Nespotřebované hodiny základní technické podpory za jednotlivé měsíce jsou převoditelné v rámci jednoho roku. Dodavatel se zavazuje, že umožní Objednateli přístup k evidenci požadavků v HelpDesku Dodavatele a uchová takto přístupné záznamy po dobu trvání této Smlouvy, minimálně do ukončení poskytování technické podpory.

11. Další podmínky poskytování technické podpory jsou uvedeny v příloze č. 1 této Smlouvy.

XIV. NÁHRADA ŠKODY

1. Každá smluvní strana je povinna nahradit škodu jí způsobenou dle platných právních předpisů a této Smlouvy. Obě smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.

2. V případě, že při činnosti prováděné Dodavatelem dojde ke způsobení škody Objednateli nebo třetím osobám, která nebude kryta pojištěním Dodavatele sjednaným dle této Smlouvy, bude Dodavatel povinen tuto škodu uhradit z vlastních prostředků.

3. Pokud v důsledku porušení povinností Dodavatele stanovených touto Smlouvou nebude Objednateli uhrazen finanční podíl nebo jeho část poskytovatelem dotace na projektu „Zajištění kybernetické bezpečnosti VOŠZ Brno, příspěvková organizace“, reg. č. projektu CZ.31.2.0/0.0/0.0/23_092/0008821, bude Dodavatel povinen uhradit Objednateli takto způsobenou škodu (celý finanční podíl, který nebude poskytovatelem dotace podle jeho rozhodnutí vyplacen, nebo který bude muset být Objednatelem vrácen).

XV. SANKCE

1. V případě prodlení Dodavatele s předáním předmětu plnění ve lhůtě dle čl. IV. odst. 5. této Smlouvy, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 10.000 Kč za každý den prodlení Dodavatele.

2. V případě prodlení Dodavatele se splněním dílčího termínu dle čl. IV. odst. 3 této Smlouvy (T1, T2, T3, T4), sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 1.000 Kč za každý den prodlení Dodavatele.

3. V případě prodlení Dodavatele se splněním povinnosti odstranit vady uvedené v protokolu o předání a převzetí plnění v ujednané lhůtě, včetně drobných vad předmětu plnění, které byly Objednatelem vytknuty, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 2.000 Kč za každý i započatý den a za každý případ prodlení (za každou vadu).

4. V případě prodlení Dodavatele s předáním zdrojového kódu, dokumentace nebo jiných souvisejících věcí dle čl. XII. odst. 11. a odst. 12. této Smlouvy, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 5.000 Kč za každý i započatý den prodlení.

5. V případě prodlení Dodavatele se splněním povinnosti zahájit řešení požadavku nahlášeného Objednatelem ve lhůtě dle čl. XIII. odst. 7. této Smlouvy (lhůta odezvy), sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši:

   5.1. 500 Kč za každou i započatou hodinu prodlení Dodavatele v případě kritického incidentu;
   5.2. 500 Kč za každou i započatou hodinu prodlení Dodavatele v případě závažného incidentu;
   5.3. 500 Kč za každý i započatý den prodlení Dodavatele v případě běžného incidentu;
   5.4. 500 Kč za každý i započatý den prodlení Dodavatele v případě minoritního incidentu.

6. V případě prodlení Dodavatele se splněním povinnosti vyřešit Objednatelem nahlášený požadavek ve lhůtě stanovené dle čl. XIII. odst. 7. této Smlouvy (lhůta vyřešení), sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši:

   6.1. 2.000 Kč za každou i započatou hodinu prodlení Dodavatele v případě kritického incidentu;
   6.2. 1.500 Kč za každý i započatý den prodlení Dodavatele v případě závažného incidentu;

6.3. 1.000 Kč za každý i započatý den prodlení Dodavatele v případě běžného incidentu;

7. V případě nesplnění povinnosti Dodavatele vést evidenci poskytování technické podpory nebo v případě prodlení s jejím předložením Objednateli sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 2.000 Kč za každý jednotlivý případ.

8. V případě:

   a) porušení povinností Dodavatele v souvislosti s užívacími právy dle této Smlouvy sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 100.000 Kč, a to za každé jednotlivé porušení takovéto povinnosti, nestanoví-li Smlouva pro určité porušení jinou smluvní pokutu;

   b) porušení povinností Dodavatele vztahujících se k ochraně osobních údajů vymezených v této Smlouvě, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 100.000 Kč, a to za každé jednotlivé porušení takovéto povinnosti;

   c) porušení povinnosti mlčenlivosti a ochrany důvěrných informací, či podmínek a požadavků na zajištění kybernetické bezpečnosti vymezených v této Smlouvě Dodavatelem, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 200.000 Kč, a to za každé jednotlivé porušení takovéto povinnosti. Za porušení povinnosti mlčenlivosti ze strany Dodavatele jsou pro účely této Smlouvy považovány i případy, kdy k porušení mlčenlivosti dojde ze strany osob, které se podílely na poskytování předmětu plnění vůči Objednateli;

9. V případě, že Dodavatel poruší své povinnosti ve vztahu k pracovněprávní ochraně svých zaměstnanců nebo zaměstnanců poddodavatele, sjednávají smluvní strany povinnost Dodavatele zaplatit Objednateli smluvní pokutu ve výši 1.000 Kč za každý zjištěný případ.

10. V případě, že Dodavatel nedodrží svou povinnost ve vztahu k pravidlům pro vzdálený přístup Dodavatele stanoveným v čl. VII. odst. 6., odst. 7., odst. 8., odst. 10. a odst. 11. této Smlouvy, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 3.000 Kč za každý jednotlivý zjištěný případ porušení této povinnosti.

11. V případě, že Dodavatel nedodrží svou povinnost předložit Objednateli kopii pojistné smlouvy nebo nebude udržovat své pojištění za podmínek stanovených v čl. VII. odst. 12. této Smlouvy, sjednávají smluvní strany ve prospěch Objednatele povinnost Dodavatele zaplatit smluvní pokutu ve výši 5.000 Kč za každý i započatý den prodlení, ve kterém nebude uvedená povinnost Dodavatele splněna.

12. Smluvní pokuty a/nebo úroky z prodlení jsou splatné na bankovní účet oprávněné smluvní strany do 14 kalendářních dnů ode dne doručení písemné výzvy oprávněné smluvní strany k jejich úhradě povinnou smluvní stranou, není-li ve výzvě uvedena lhůta delší.

13. Úhrada jakékoliv smluvní pokuty nezbavuje Dodavatele povinnosti splnit své závazky ze Smlouvy, ani jí není dotčen nárok Objednatele na náhradu škody v plné výši, ani povinnost Dodavatele bezodkladně odstranit závadný stav.

XVI. OCHRANA OSOBNÍCH ÚDAJŮ

1. Dodavatel prohlašuje, že si je vědom, že Objednatel jako správce osobních údajů ve smyslu nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) zpracovává osobní údaje Dodavatele, jeho zaměstnanců či členů orgánů a osobní údaje poddodavatelů Dodavatele, jejich zaměstnanců a členů orgánů (vše společně dále jen „osobní údaje") pro účely plnění povinností vyplývajících ze zákona, plnění závazků podle této Smlouvy nebo oprávněných zájmů Objednatele.
2. Objednatel prohlašuje, že veškeré osobní údaje, které Dodavatel poskytne Objednateli nebo se kterými přijde Objednatel do styku v souvislosti s plněním závazku podle této Smlouvy, nebudou využívány k jiným účelům, než k jakým byly Dodavatelem Objednateli poskytnuty nebo Objednatelem pro účely plnění této Smlouvy shromážděny.
3. Dodavatel se zavazuje chránit veškeré osobní údaje, které mu budou poskytnuty, zpřístupněny či se kterými přijde do styku v souvislosti s plněním předmětu této Smlouvy.

XVII. OCHRANA INFORMACÍ, KYBERNETICKÁ BEZPEČNOST

1. Smluvní strany jsou si vědomy toho, že v rámci plnění závazků z této Smlouvy:
    a) si mohou vzájemně vědomě nebo opomenutím poskytnout informace, které budou považovány za důvěrné (dále jen „**důvěrné informace**“);
    b) mohou jejich zaměstnanci a osoby v obdobném postavení získat vědomou činností druhé smluvní strany nebo i jejím opomenutím přístup k důvěrným informacím a osobním údajům druhé smluvní strany.
2. Smluvní strany se zavazují, že žádná z nich bez písemného souhlasu druhé smluvní strany nezpřístupní třetí osobě důvěrné informace, které získala při plnění této Smlouvy, ani je nepoužije v rozporu s účelem této Smlouvy.
3. Veškeré informace, které Dodavatel při plnění této Smlouvy získá od Objednatele nebo o Objednateli či jeho zaměstnancích a spolupracovnících, se považují za důvěrné, není-li stanoveno jinak. Veškeré informace poskytnuté Dodavatelem Objednateli se považují za důvěrné, pouze pokud na jejich důvěrnost Dodavatel Objednateli předem písemně upozornil a Objednatel Dodavateli písemně potvrdil svůj závazek důvěrnost těchto informací zachovávat.
4. Veškeré důvěrné informace zůstávají výhradním vlastnictvím předávající smluvní strany a přijímající smluvní strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní důvěrné informace. S výjimkou rozsahu, který je nezbytný pro plnění této Smlouvy, se obě smluvní strany zavazují neduplikovat žádným způsobem důvěrné informace druhé smluvní strany, nepředat je třetí straně ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli plnit tuto Smlouvu. Obě smluvní strany se zároveň zavazují nepoužít důvěrné informace druhé smluvní strany jinak než za účelem plnění této Smlouvy.
5. Bez ohledu na jiná ustanovení této Smlouvy je Objednatel povinen uveřejnit na příslušných webových stránkách v souladu se ZZVZ či zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých

smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů:

a) tuto Smlouvu včetně všech jejích změn a dodatků;

b) výši skutečně uhrazené ceny za plnění veřejné zakázky.

6. Dodavatel se zavazuje k zachování bezpečnosti informací a dat obsažených v informačních systémech spravovaných Objednatelem, včetně jiných informačních systémů, které budou plněním smlouvy dotčeny, a to zejm. z pohledu důvěrnosti, dostupnosti a integrity. Dodavatel je povinen při provádění díla jednat tak, aby důvěrnost, dostupnost a integrita informací a dat dle předchozí věty nebyla přerušena, ohrožena, ani omezena. Je-li k plnění dle smlouvy nezbytné důvěrnost, dostupnost či integritu dat omezit, ohrozit nebo přerušit, Dodavatel tak učiní pouze po předchozí dohodě s Objednatelem a jen v Objednatelem odsouhlaseném rozsahu.

7. Dodavatel je povinen v průběhu realizace plnění dle této Smlouvy průběžně poskytovat součinnost při identifikaci významných změn a jejich dopadů do oblasti kybernetické bezpečnosti Objednatele. V případě identifikace významných změn souvisejících s realizací plnění se Poskytovatel zavazuje spolupracovat s Objednatelem na identifikaci potencionálních rizik možných dopadů významných změn a v případě potřeby poskytne Objednateli informace o možných opatřeních pro snížení nepříznivých možných dopadů spojených s významnými změnami.

8. V případě výskytu kybernetického bezpečnostního incidentu, který souvisí s realizací plnění, je Dodavatel povinen o něm Objednatele neprodleně písemně informovat, a to nejpozději do následujícího dne po zjištění kybernetického bezpečnostního incidentu. Toto hlášení bude identifikovat konkrétní část předmětu plnění, kde ke kybernetickému bezpečnostnímu incidentu došlo, dále sdělení, kdy k němu došlo, a zejména popis tohoto incidentu. Smluvní strany následně budou spolupracovat na řešení incidentu a na nápravných opatřeních, tak aby byla minimalizována rizika z incidentu vyplývající.

9. Dodavatel se bude řídit bezpečnostní politikou a předpisy Objednatele, se kterými byl Objednatelem seznámen a které souvisí s plněním dle smlouvy.

XVIII. SOUČINNOST A EXTERNÍ KONTROLA

1. Dodavatel se zavazuje poskytnout Objednateli potřebnou součinnost při výkonu finanční kontroly dle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů.

2. Dodavatel uchová veškerou dokumentaci a účetní doklady související s plněním podle této Smlouvy minimálně do 31.12.2036. Pokud je v českých právních předpisech stanovena lhůta delší než v evropských předpisech, musí být použita pro úschovu delší lhůta, a to i delší než lhůta ujednaná tímto odstavcem Smlouvy.

3. Dodavatel je povinen minimálně do 31. 12. 2036 poskytovat sám či prostřednictvím Objednatele požadované informace a dokumentaci (včetně účetních dokladů) související s realizací projektu zaměstnancům nebo zmocněncům pověřených orgánů (OLAF – Evropský úřad pro boj proti podvodům, Úřad evropského veřejného žalobce, Ministerstva financí ČR, Evropské komise, Evropského účetního dvora, Ministerstva vnitra ČR, Nejvyššího kontrolního úřadu a dalším příslušným vnitrostátním orgánům), a je povinen vytvořit výše uvedeným subjektům podmínky k provedení kontroly vztahující se k realizaci

projektu a poskytnout jim při provádění kontroly součinnost. Náklady související s těmito kontrolami a poskytováním informací a součinnosti jsou zahrnuty do ceny díla.

XIX. ROZHODNÉ PRÁVO

1. Vztahy mezi smluvními stranami touto Smlouvou výslovně neupravené se budou řídit obecně závaznými právními předpisy České republiky, zejména občanským zákoníkem a příslušnými právními předpisy souvisejícími.
2. Veškeré spory mezi smluvními stranami vyplývající z této Smlouvy nebo z jejího porušení, ukončení nebo neplatnosti budou rozhodovány věcně a místně příslušnými soudy České republiky dle sídla Objednatele, pokud nebudou vyřešeny dohodou obou smluvních stran.

XX. ZÁVĚREČNÁ USTANOVENÍ

1. Tato Smlouva nabývá platnosti dnem podpisu obou smluvních stran, účinnosti nabývá okamžikem zveřejněním Smlouvy v registru smluv podle zákona č. 340/2015 Sb., o registru smluv. Uveřejnění Smlouvy v registru smluv zajistí Objednatel, o čemž bezodkladně vyrozumí Dodavatele.
2. Tato Smlouva představuje úplnou dohodu smluvních stran o předmětu této Smlouvy. Tuto Smlouvu je možné měnit pouze písemnou dohodou smluvních stran ve formě vzestupně číslovaných dodatků této Smlouvy uzavřených v souladu s příslušnými ustanoveními občanského zákoníku, popř. obdobných předpisů tyto předpisy nahrazujících, a podepsaných osobami oprávněnými jednat jménem smluvních stran.
3. Smluvní strany si nepřejí, aby nad rámec výslovných ustanovení této Smlouvy byla jakákoliv práva a povinnosti dovozována z dosavadní či budoucí praxe zavedené mezi smluvními stranami či zvyklostí zachovávaných obecně či v odvětví týkajícím se předmětu plnění této Smlouvy, ledaže je v této Smlouvě výslovně sjednáno jinak. Vedle shora uvedeného si smluvní strany potvrzují, že si nejsou vědomy žádných dosud mezi nimi zavedených obchodních zvyklostí či praxe.
4. Smluvní strany se podpisem této Smlouvy dohodly, že vylučují aplikaci ustanovení § 557 občanského zákoníku.
5. Pro vyloučení pochybností Dodavatel výslovně potvrzuje, že je podnikatelem, uzavírá tuto Smlouvu při svém podnikání, a na tuto Smlouvu se tudíž neuplatní ustanovení § 1793 občanského zákoníku.
6. Dodavatel na sebe v souladu s ustanovením § 1765 odst. 2 občanského zákoníku přebírá nebezpečí změny okolností. Tímto však nejsou nikterak dotčena práva smluvních stran upravená v této Smlouvě.
7. Je-li nebo stane-li se jakékoli ustanovení této Smlouvy neplatným, nezákonným nebo nevynutitelným, netýká se tato neplatnost a nevynutitelnost zbývajících ustanovení této Smlouvy. Smluvní strany se tímto zavazují nahradit do 10-ti pracovních dnů po doručení výzvy druhé smluvní strany jakékoli takové neplatné, nezákonné nebo nevynutitelné ustanovení ustanovením, které je platné, zákonné a vynutitelné a má stejný nebo alespoň podobný obchodní a právní význam.
8. Veškerá práva a povinnosti vyplývající z této Smlouvy přecházejí, pokud to povaha těchto práv a povinností nevylučuje, na právní nástupce smluvních stran.

9. Dodavatel není oprávněn započítat, zastavit ani postoupit žádné své peněžité nároky vůči Objednateli vzniklé na základě této Smlouvy na třetí osobu bez předchozího písemného souhlasu Objednatele.
10. Dodavatel se zavazuje, že bez předchozího výslovného písemného souhlasu Objednatele nepostoupí třetí straně tuto Smlouvu nebo jakoukoli její část nebo jakékoli právo či závazek z této Smlouvy vyplývající. Toto ustanovení se nevztahuje na případné právní nástupce smluvních stran.
11. Tato Smlouva je uzavřena elektronickou formou s využitím kvalifikovaných elektronických podpisů osob oprávněných právně jednat v zastoupení smluvních stran.
12. Smluvní strany prohlašují, že tato Smlouva je projevem jejich pravé a svobodné vůle a na důkaz dohody o všech článcích této Smlouvy připojují své podpisy.
13. Nedílnou součástí této Smlouvy jsou:

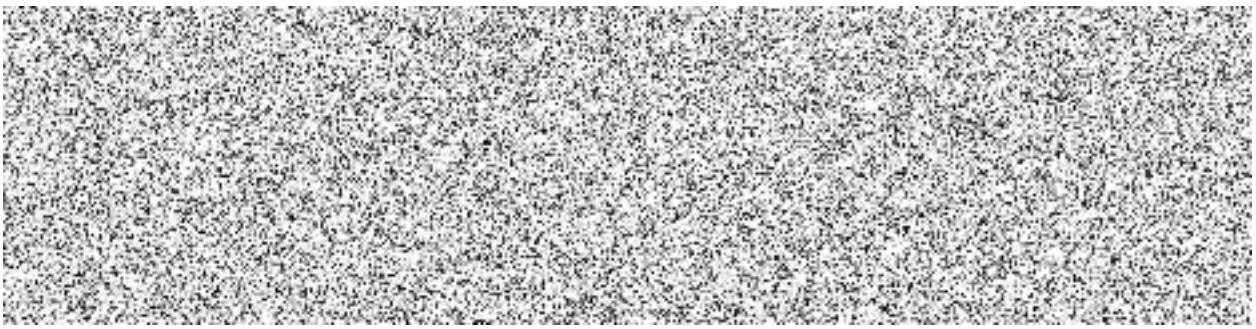
    Příloha č. 1 – Technická specifikace a popis nabízeného řešení

    Příloha č. 2 – Cenová nabídka

    Příloha č. 3 – Realizační tým

    Příloha č. 4 – Seznam poddodavatelů

Za Objednatele	Za Dodavatele
V Brně dne dle data el. podpisu	V Brně dne dle data el. podpisu



Technická specifikace plnění

Obsah

Popis projektu a společná kritéria

Projekt je koncipován jako ucelené řešení bezpečnosti Zadavatele, nikoliv jako dodávka technologií. Skládá se z následujících provázaných celků:

- Technologie – souhrn řešení pro jednotlivé oblasti bezpečnosti, jež je tvořena konkrétními produkty s výkonnostními parametry.
- Integrace – způsob kooperace a míra provázanosti technologií tak, aby tvořily funkční celek s maximální přidanou hodnotou pro bezpečnost daného prostředí.

Ke každé technologii (aktivitě) bude vypracován Cílový koncept (Solution Design dokument), který popíše přesné zapojení do stávající infrastruktury, popis systémové konfigurace a provozní konfigurace, včetně integrací a veškeré interoperability s dalšími technologiemi. Nastavení konfigurace a uvedení do ostrého provozu musí být rozplánováno s ohledem na kapacitní možnosti Zadavatele, případně servisní okna daného prostředí dle dopadů na funkcionalitu. Solution Design musí být vzájemně odsouhlasen.

Konfigurační parametry dané definicí procesů a opatření musí být následně aplikovány na všechny technologie v rámci dodávky projektu a dále na existující technologie, které to dovolují (např. komunikační protokoly včetně úrovně zabezpečení, síla hesla, atp.).

DR (Disaster Recovery) plán jakožto jeden z poptávaných výstupů v rámci analytických prací definuje participaci jednotlivých technologií při obnově primárních procesů organizace a určuje formu a rychlost obnovy chodu technologie. Toto musí být reflektováno v popisu obnov technologií a jejich návazností formou detailní provozní dokumentace. Pro účely DR je dále požadováno, aby měly všechny dotčené systémy nastaven adekvátní plán zálohování dat a systémové konfigurace, přičemž bude podle připravených scénářů docházet k pravidelným testům obnovy. Podle typu řešení lze využít formu snapshotu ve virtuálním prostředí, automatického provisioning procesu skrze automatizační scripty a šablony, případně rekonfigurace HW zařízení přes OOB (out of band) rozhraní.

Schopnost dané technologie zajistit konzistenci systémové konfigurace a procesovaných dat při zálohování a obnově je společným požadovaným kritériem pro všechny technologie v rámci dodávky.

Všechny technologie využívající certifikáty musí používat Public Key Infrastructure (PKI) definovanou v rámci projektu, přičemž je vyžadován standard TLS 1.2 či vyšší.

Všechny nově pořizované technologie projektu musí být pokryty podporou od výrobce po dobu minimálně 60měsíců, a to v režimu NBD 5x8; preferovány jsou trvalé (perpetual) licence, v případě, že trvalá licence není k dispozici, pak subscription s plnou funkcionalitou na dobu minimálně 60 měsíců.

V případě potřeby pořízení dodatečných licencí po dobu nezbytně nutnou pro účely implementace/testování, musí být tyto součástí nabídky dodavatele a řádně naceněny v rámci položkového rozpočtu na separátním řádku jako samostatná položka.

ID001 - Zabezpečení síťové infrastruktury (NAC/802.1x) + Zabezpečení perimetru NGFW

Základní obecný prvek bezpečnosti je nasazení NGFW, který doposud ve škole není nasazen. Zvýší se obecně bezpečnost pro všechny IS ve škole. NAC + 802.1x zajistí bezpečný provoz všech IS ve škole, díky zcela jasně dané definici přistupujících uživatelů do dítě, dojde ke zvýšení bezpečnosti a ochrany IS. Pro použití IS je zcela kruciální dobré síťové prostředí, které díky nasazení nových aktivních prvků a technologií tento stav zajistí. Páteřní propojení budou posíleny z 1G na 10Gb a uživatelsky na 1Gb

Firewall technologie

NGFW		
Požadovaný počet : 2		
Název a výrobce	**Výrobce: Fortinet** **Název: FortiGate 91G + UTP**	
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
HW appliance o maximální velikosti 1U	ANO	HW appliance o maximální velikosti 1U
Podpora režimu vysoké dostupnosti active/active a active/passive	ANO	Podpora režimu vysoké dostupnosti active/active a active/passive
Podpora duálního napájení (dva zdroje a přívodní kabeláž je součástí každého dodaného zařízení)	ANO	Podpora duálního napájení (dva zdroje a přívodní kabeláž je součástí každého dodaného zařízení)
Minimálně 2x 10 GbE SFP+	ANO	Minimálně 2x 10 GbE SFP+
Minimálně 8x 1 GbE RJ45 síťová rozhraní	ANO	Minimálně 8x 1 GbE RJ45 síťová rozhraní
lokální úložiště min 100GB založené na nerotační technologii (SSD disk)	ANO	lokální úložiště min 100GB založené na nerotační technologii (SSD disk)

Integrované TPM řešení nebo jeho ekvivalent	ANO	Integrované TPM řešení nebo jeho ekvivalent
Výkonové požadavky	ANO/NE	Výkonové požadavky
Minimální propustnost NGFW pro IPv4 provoz je 25 Gbps (UDP komunikace a paket velikosti 512B)	ANO	Minimální propustnost NGFW pro IPv4 provoz je 25 Gbps (UDP komunikace a paket velikosti 512B)
Kapacita současně navázaných spojení NGFW je alespoň 3 000 000 a kapacita nově sestavených spojení za sekundu je alespoň 120 000	ANO	Kapacita současně navázaných spojení NGFW je alespoň 3 000 000 a kapacita nově sestavených spojení za sekundu je alespoň 120 000
Propustnost NGFW pro IPSEC VPN je alespoň 25 Gbps bez licenčního omezení počtu sestavených spojení	ANO	Propustnost NGFW pro IPSEC VPN je alespoň 25 Gbps bez licenčního omezení počtu sestavených spojení
Propustnost NGFW při zapnuté funkci SSL inspekce využívající IPS inspekci je alespoň 2,5 Gbps	ANO	Propustnost NGFW při zapnuté funkci SSL inspekce využívající IPS inspekci je alespoň 2,5 Gbps
Propustnost NGFW při zapnuté funkci aplikační kontroly je alespoň 6,5 Gbps	ANO	Propustnost NGFW při zapnuté funkci aplikační kontroly je alespoň 6,5 Gbps
Propustnost NGFW při zapnuté funkci IPS inspekce a současném logování provozu je alespoň 4 Gbps	ANO	Propustnost NGFW při zapnuté funkci IPS inspekce a současném logování provozu je alespoň 4 Gbps
Propustnost NGFW při paralelně provozovaných funkcích stavového FW, IPS, aplikační kontrole a logovaní (obecně popisovaná kombinace funkcí pro NGFW zařízení) je alespoň 2 Gbps	ANO	Propustnost NGFW při paralelně provozovaných funkcích stavového FW, IPS, aplikační kontrole a logovaní (obecně popisovaná kombinace funkcí pro NGFW zařízení) je alespoň 2 Gbps
Maximální udávaná latence NGFW (pro UDP provoz nebo průměrná hodnota) je 9 µs	ANO	Maximální udávaná latence NGFW (pro UDP

		provoz nebo průměrná hodnota) je 9 µs
Funkční požadavky	ANO/NE	Funkční požadavky
Jedná se o řešení dnes označované jako NGFW s integrovanou grafickou a CLI správou umožňující kompletní obsluhu zařízení	ANO	Jedná se o řešení dnes označované jako NGFW s integrovanou grafickou a CLI správou umožňující kompletní obsluhu zařízení
Podpora stavového firewallingu pro IPv4 i IPv6, podpora nat 64/46	ANO	Podpora stavového firewallingu pro IPv4 i IPv6, podpora nat 64/46
Podpora režimů explicitní a transparentní proxy	ANO	Podpora režimů explicitní a transparentní proxy
Podpora ověřování identity uživatelů pomocí externích zdrojů s možností napojení na MS Active Directory, LDAP, Radius, Kerberos a práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On	ANO	Podpora ověřování identity uživatelů pomocí externích zdrojů s možností napojení na MS Active Directory, LDAP, Radius, Kerberos a práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On
Podpora lokální databáze a vzdálené databáze (radius, ldap, tacacs+, saml, kerberos) pro ověřování uživatelů	ANO	Podpora lokální databáze a vzdálené databáze (radius, ldap, tacacs+, saml, kerberos) pro ověřování uživatelů
Ověřování uživatelů pomocí SSO funkcionality pomocí Radius Single Sign On a AD pollingu	ANO	Ověřování uživatelů pomocí SSO funkcionality pomocí Radius Single Sign On a AD pollingu
Funkce QoS, traffic shaping a SD-WAN minimálně v režimu vytvoření overlay a underlay virtuálních sítových rozhraní zahrnující fyzické propoje, IPSEC tunely či jiná rozhraní s možností definice pravidel pro řízení směrování, strategie využívání jednotlivých linek současně a monitorování stavu jednotlivých linek	ANO	Funkce QoS, traffic shaping a SD-WAN minimálně v režimu vytvoření overlay a underlay virtuálních sítových rozhraní zahrnující fyzické propoje, IPSEC tunely či jiná rozhraní s možností definice pravidel pro řízení směrování, strategie využívání jednotlivých

		linek současně a monitorování stavu jednotlivých linek
Podpora funkcí VPN brány - IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran); - SSL VPN pro klientský přístup s podporou tunelového režimu včetně zdarma dostupného klienta pro osobní počítače i mobilní platformy a zároveň NGFW podporuje portálový režim pro bezklientský přístup.	ANO	Podpora funkcí VPN brány - IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran); - SSL VPN pro klientský přístup s podporou tunelového režimu včetně zdarma dostupného klienta pro osobní počítače i mobilní platformy a zároveň NGFW podporuje portálový režim pro bezklientský přístup.
Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3	ANO	Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3
Možnost logické segmentace zařízení s použitím tzv. virtuálních kontextů v minimálním počtu deseti současně běžících kontextů v ceně zařízení; každý virtuální kontext musí pracovat izolovaně. Řešení umožňuje interně propojit jednotlivé logické kontexty na úrovni L2 (sdílení broadcast domény) i L3 včetně NGFW inspekce provozu mezi kontexty.	ANO	Možnost logické segmentace zařízení s použitím tzv. virtuálních kontextů v minimálním počtu deseti současně běžících kontextů v ceně zařízení; každý virtuální kontext umí pracovat izolovaně. Řešení umožňuje interně propojit jednotlivé logické kontexty na úrovni L2 (sdílení broadcast domény) i L3 včetně NGFW inspekce provozu mezi kontexty.
Antivirový engine musí být vybaven lokální databází vzorků škodlivého kódu a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků	ANO	Antivirový engine je vybaven lokální databází vzorků škodlivého kódu a AI/ML enginem pro

		identifikaci podezřelých či neznámých vzorků
Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných kancelářských dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora napojení na sandboxovací funkce včetně funkce akceptace lokálních signaturových databází generovaných sandboxem, vše bez nutnosti instalace pluginů do prohlížeče.	ANO	Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných kancelářských dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora napojení na sandboxovací funkce včetně funkce akceptace lokálních signaturových databází generovaných sandboxem, vše bez nutnosti instalace pluginů do prohlížeče.
Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 4000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace	ANO	Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 4000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace

		rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace
Možnost definice zakázaných slov pro vyhledávání na internetu	ANO	Možnost definice zakázaných slov pro vyhledávání na internetu
Schopnost inspekce protokolu QUIC	ANO	Schopnost inspekce protokolu QUIC
Možnost využít výrobcem udržovanou databázi internetových služeb při definici bezpečnostní politiky	ANO	Možnost využít výrobcem udržovanou databázi internetových služeb při definici bezpečnostní politiky
Podpora kategorizace streamovaných videí a kanálů jako například YouTube	ANO	Podpora kategorizace streamovaných videí a kanálů jako například YouTube
Podpora ZTNA bezpečného přístupu	ANO	Podpora ZTNA bezpečného přístupu
Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovanýANOmální filtr a mechanismus kontroly validity vybraných protokolů	ANO	Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovanýANOmální filtr a mechanismus kontroly validity vybraných protokolů
Možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), GeoIP databáze, data a času	ANO	Možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), GeoIP databáze, data a času

Podpora dvoufaktorové autentizace pomocí HW nebo mobilních OTP tokenů, součástí nabídky musí být alespoň jeden testovací HW/mobilní token a plně funkční řešení dvoufaktorového OTP ověřování uživatelů pro administrátory a uživatele VPN	ANO	Podpora dvoufaktorové autentizace pomocí HW nebo mobilních OTP tokenů, součástí nabídky je alespoň jeden testovací HW/mobilní token a plně funkční řešení dvoufaktorového OTP ověřování uživatelů pro administrátory a uživatele VPN
Podpora režimu nasazení v režimu WCCP (WCCP v2)	ANO	Podpora režimu nasazení v režimu WCCP (WCCP v2)
Podpora konfiguračních PAC souborů pro režim nasazení explicitní proxy	ANO	Podpora konfiguračních PAC souborů pro režim nasazení explicitní proxy
Podpora ICAP rozhraní pro obousměrnou integraci s externími servery	ANO	Podpora ICAP rozhraní pro obousměrnou integraci s externími servery
Podpora tunelování provozu pomocí technologií GRE a VxLAN (NGFW funguje jako VTEP)	ANO	Podpora tunelování provozu pomocí technologií GRE a VxLAN (NGFW funguje jako VTEP)
Podpora statického a dynamického směrování minimálně protokoly OSPF a BGP ve verzí IPv4 a IPv6	ANO	Podpora statického a dynamického směrování minimálně protokoly OSPF a BGP ve verzí IPv4 a IPv6
Podpora Policy Based Routing na základě IP adresy a aplikace (s možností definovat vlastní aplikace)	ANO	Podpora Policy Based Routing na základě IP adresy a aplikace (s možností definovat vlastní aplikace)
Podpora IPAM funkcionality pro správu přidělených IP adres z NGFW zařízení	ANO	Podpora IPAM funkcionality pro správu přidělených IP adres z NGFW zařízení
Podpora automaticky aktivovaného bypass režimu v případě přetížení systému a jeho inspekčních funkcí	ANO	Podpora automaticky aktivovaného bypass režimu v případě přetížení systému a jeho inspekčních funkcí

funkce ochrany proti DDoS útoku na zařízení alespoň v podobě nastavení limitu objemu a typu provozu, který bude zařízení aktivně zpracovávat před jeho zahozením	ANO	funkce ochrany proti DDoS útoku na zařízení alespoň v podobě nastavení limitu objemu a typu provozu, který bude zařízení aktivně zpracovávat před jeho zahozením
Analýza a zabezpeční DNS dotazů (ochrana před DNS poisoningem), filtrování DNS dotazů na základě kategorizace	ANO	Analýza a zabezpeční DNS dotazů (ochrana před DNS poisoningem), filtrování DNS dotazů na základě kategorizace
Možnost filtrovat Java applety, ActiveX prvky, Cookie soubory ve webovém provozu	ANO	Možnost filtrovat Java applety, ActiveX prvky, Cookie soubory ve webovém provozu
NGFW může zároveň plnit funkci bezdrátového kontroleru pro bezdrátové přístupové body od stejného výrobce	ANO	NGFW může zároveň plnit funkci bezdrátového kontroleru pro bezdrátové přístupové body od stejného výrobce
Integrovaná funkce load balancingu (reverzní proxy) s podporou základní algoritmů pro rozklad zátěže (Round-robin, váhování, nejkratší odezva, nejmenší počet aktivních spojení) s detekcí stavu reálných serverů na pozadí, podpora funkce ssl offloading a ssl inspekce pro rozkládaný provoz	ANO	Integrovaná funkce load balancingu (reverzní proxy) s podporou základní algoritmů pro rozklad zátěže (Round-robin, váhování, nejkratší odezva, nejmenší počet aktivních spojení) s detekcí stavu reálných serverů na pozadí, podpora funkce ssl offloading a ssl inspekce pro rozkládaný provoz
Další požadavky	ANO/NE	Další požadavky
Součástí každého dodaného zařízení je podpora výrobce s možností kontaktovat podporu 24/7, vyměnit zařízení v režimu 8x5, licence pro spuštění požadovaných funkcí a výrobce umožňuje zdarma stáhnout VPN klienta kompatibilního s nabízeným NGFW. Vše s platností 5 let.	ANO	Součástí každého dodaného zařízení je podpora výrobce s možností kontaktovat podporu 24/7, vyměnit zařízení v režimu 8x5, licence pro spuštění požadovaných funkcí a výrobce umožňuje zdarma

		stáhnout VPN klienta kompatibilního s nabízeným NGFW. Vše s platností 5 let.

implementace

NGFW - implementace		
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
fyzická montáž zařízení a propojení do stávající síťové infrastruktury	ANO	fyzická montáž zařízení a propojení do stávající síťové infrastruktury
upgrade firmware na aktuální stabilní verzi doporučenou výrobcem	ANO	upgrade firmware na aktuální stabilní verzi doporučenou výrobcem
analýza stavu topologie a současné konfigurace	ANO	analýza stavu topologie a současné konfigurace
zapojení do clusteru, včetně možnosti rozložení zátěže na jednotlivé boxy	ANO	zapojení do clusteru, včetně možnosti rozložení zátěže na jednotlivé boxy
úprava konfigurace firewallu dle doporučení vyplívající z analýzy	ANO	úprava konfigurace firewallu dle doporučení vyplívající z analýzy
optimalizace bezpečnostních profilů	ANO	optimalizace bezpečnostních profilů
migrace konfigurace všech funkcionalit implementovaných na stávajících firewallech včetně WiFi kontroléru	ANO	migrace konfigurace všech funkcionalit implementovaných na stávajících firewallech včetně WiFi kontroléru
konfigurace hloubkové SSL inspekce	ANO	konfigurace hloubkové SSL inspekce
akceptační testy a testovací provoz	ANO	akceptační testy a testovací provoz
školení administrátorů v rozsahu 4 hodin	ANO	školení administrátorů v rozsahu 4 hodin
dokumentace skutečného provedení	ANO	dokumentace skutečného provedení
rekonfigurace RDS, která byla pozdržena do doby upgrade centrálních firewallů	ANO	rekonfigurace RDS, která byla pozdržena do doby upgrade centrálních firewallů
návrh topologie SD-WAN	ANO	návrh topologie SD-WAN
konfigurace SD-WAN, dynamic routing (BGP, OSPF) v centru	ANO	konfigurace SD-WAN, dynamic routing (BGP, OSPF) v centru
konfigurace SD-WAN, dynamic routing (BGP, OSPF) vzdálených lokalit, rekonfigurace fw pravidel	ANO	konfigurace SD-WAN, dynamic routing (BGP, OSPF) vzdálených lokalit, rekonfigurace fw pravidel
implementace management nástroje a napojení všech prvků do managementu	ANO	implementace management nástroje a napojení všech prvků do managementu

Aktivní prvky core switch a POE switch

Cílem je modernizace počítačové sítě náhradou zastaralých prvků a zvýšení její kapacity doplněním nových prvků. Současně bude pro zvýšení úrovně zabezpečení počítačové sítě implementován systém řízení přístupu k síti NAC na bázi protokolu IEEE 802.1X s napojením na centrální databázi identit Active Directory. NAC bude implementován jako jednotný pro drátovou i bezdrátovou část sítě a dynamické zařazování koncových zařízení do VLAN na základě ověření, typu zařízení apod.

Management A Obecné technické požadavky

management platforma přepínačů		
Obecné požadavky na management platformu přepínače	ANO/NE	Popis splnění požadavku
Efektivní správa poptávaných přepínačů z hlediska konfigurace, zabezpečení, logování, atd. pro zefektivnění jejich nasazení a následné správy	ANO	Efektivní správa poptávaných přepínačů z hlediska konfigurace, zabezpečení, logování, atd. pro zefektivnění jejich nasazení a následné správy
Může se jednat o fyzické i VM řešení (pro platformu ESXi)	ANO	Může se jednat o fyzické i VM řešení (pro platformu ESXi)
Management platforma musí umožnit grafické znázornění fyzické a logické topologie spravovaných přepínačů	ANO	Management platforma umožnuje grafické znázornění fyzické a logické topologie spravovaných přepínačů
Management platforma musí umožnit zobrazení a vyhledávání koncových zařízení připojených ke spravovaným zařízením ve fyzické i logické topologii	ANO	Management platforma umožnuje zobrazení a vyhledávání koncových zařízení připojených ke spravovaným zařízením ve fyzické i logické topologii
Management platforma musí umožnit automatickou zálohu konfigurace přepínačů a možnost její migrace na nový přepínač v případě výměny přepínače	ANO	Management platforma umožnuje automatickou zálohu konfigurace přepínačů a možnost její migrace na nový přepínač v případě výměny přepínače
Management platforma musí umožnit poskytnout údaje o vytížení jednotlivých přepínačů jak z pohledu CPU a paměti, tak datových toků na jednotlivých portech	ANO	Management platforma umožnuje poskytnout údaje o vytížení jednotlivých přepínačů jak z pohledu CPU a paměti, tak datových toků na jednotlivých portech
Management platforma musí umožnit kompletní síťovou i bezpečnostní konfiguraci přepínačů	ANO	Management platforma umožnuje kompletní síťovou i bezpečnostní konfiguraci přepínačů
Management platforma musí umožnit spravovat karanténu koncových zařízení vyvolanou administrátorem nebo automaticky na základě bepzčnostního incidentu	ANO	Management platforma umožnuje spravovat karanténu koncových zařízení vyvolanou administrátorem nebo automaticky na základě bepzčnostního incidentu
Management platforma musí umožnit hromadnou správu více přepínačů najednou pro akce jako je například upgrade jejich operačního systému a registrace jejich podpory	ANO	Management platforma umožnuje hromadnou správu více přepínačů najednou pro akce jako je například upgrade jejich operačního systému a registrace jejich podpory. Lze udělat hromadný upgrade z GUI/CLI postupný. .Hromadná registrace

		podpory lze pomocí založení ticketu na supportu
Management platforma musí umožnit administrátorský přístup pomocí SSH a HTTPS a také z ní je možné SSH přístup na samotné přepínače	ANO	Management platforma umožnuje administrátorský přístup pomocí SSH a HTTPS a také z ní je možné SSH přístup na samotné přepínače
Management platforma musí umožnit použití REST API pro konfiguraci a monitoring systému	ANO	Management platforma umožnuje použití REST API pro konfiguraci a monitoring systému
Management platforma musí podporovat SNMP v1/v2c/v3 a Syslog včetně nativní integrace s poptávaným analyzátorem provozu	ANO	Management platforma musí podporovat SNMP v1/v2c/v3 a Syslog včetně nativní integrace s poptávaným analyzátorem provozu
Management platforma musí umožnit RBAC pro administrátorský přístup	ANO	Management platforma umožnuje RBAC pro administrátorský přístup

Obecné technické požadavky na poptávané přepínače		
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
Podpora IEEE 802.3ad	ANO	Podpora IEEE 802.3ad
Podpora IEEE 802.1q	ANO	Podpora IEEE 802.1q
Podpora IEEE 802.1ab	ANO	Podpora IEEE 802.1ab
Možnost propojení s prvkem podporující IEEE 802.1s	ANO	Možnost propojení s prvkem podporující IEEE 802.1s
Podpora IEEE 802.1w	ANO	Podpora IEEE 802.1w
Podpora 802.1x	ANO	Podpora 802.1x
Podpora MAB	ANO	Podpora MAB
Podpora Radius CoA	ANO	Podpora Radius CoA
Podpora Radius Accounting	ANO	Podpora Radius Accounting
Podpora ARP inspekce	ANO	Podpora ARP inspekce
Podpora IGMP a DHCP snooping	ANO	Podpora IGMP a DHCP snooping
Podpora Jumbo Frame o velikosti alespoň 9000B	ANO	Podpora Jumbo Frame o velikosti alespoň 9000B
Podpora SPAN	ANO	Podpora SPAN

Podpora administrátorského přístupu pomocí Telnet, SSH a HTTPS	ANO	Podpora administrátorského přístupu pomocí Telnet, SSH a HTTPS
Podpora REST API pro konfiguraci a monitoring prvku	ANO	Podpora REST API pro konfiguraci a monitoring prvku
Podpora SNMP v1/v2c/v3, Syslog (včetně možnosti komunikace pomocí TCP), Radius a TACACS+ protokolu pro autentizaci administrátorů	ANO	Podpora SNMP v1/v2c/v3, Syslog (včetně možnosti komunikace pomocí TCP), Radius a TACACS+ protokolu pro autentizaci administrátorů
Podpora centrální správy z NGFW zařízení stejného výrobce s možností vynutit L2 inspekci provozu přes NGFW per VLAN	ANO	Podpora centrální správy z NGFW zařízení stejného výrobce s možností vynutit L2 inspekci provozu přes NGFW per VLAN

Core přepínače

přepínače s 24 porty		
Požadovaný počet : 2		
Název a výrobce	**Výrobce: FORTINET** **Název: FortiSwitch-624F + 5 Year FortiCare Premium Support**	
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
Minimálně 24x 1GE/2.5GE/5GE RJ45 ports a 4x 10GE/25GE SFP+/SFP28 port	ANO	Minimálně 24x 1GE/2.5GE/5GE RJ45 ports a 4x 10GE/25GE SFP+/SFP28 port
Samostatný konzolový port, L3 mgmt port a USB port	ANO	Samostatný konzolový port, L3 mgmt port a USB port
Velikost maximálně 1RU	ANO	Velikost maximálně 1RU
Minimální přepínací kapacita 440 Gbps	ANO	Minimální přepínací kapacita 440 Gbps
Propustnost minimálně 654 Mpps	ANO	Propustnost minimálně 654 Mpps
Velikost bufferu pro zpracování paketů je alespoň 8 MB per port	ANO	Velikost bufferu pro zpracování paketů je alespoň 8 MB per port
Minimální velikost MAC tabulky alespoň 62000 záznamů	ANO	Minimální velikost MAC tabulky alespoň 62000 záznamů
Minimální počet podporovaných VLAN alespoň 4000	ANO	Minimální počet podporovaných VLAN alespoň 4000
Požadavky na podporu přepínačů výrobcem	ANO/NE	Popis splnění požadavku
Nativní podpora HW výrobce s možností výměny vadného HW do třiceti dnů a to až pět let po ohlášení konce možnosti objednat nabízený přepínač	ANO	Nativní podpora HW výrobce s možností výměny vadného HW do třiceti dnů a to až pět let po ohlášení konce možnosti objednat nabízený přepínač
Podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 a možnost výměny vadného zařízení v režimu 8x5. Obojí po dobu 5 let.	ANO	Podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 a možnost výměny vadného zařízení v režimu 8x5. Obojí po dobu 5 let.

přepínače s 48 porty s PoE

přepínače s 48 porty s PoE		
Požadovaný počet : 7		
Název a výrobce	**Výrobce: FORTINET Název: FortiSwitch-148F-FPOE + 5 Year FortiCare Premium Support**	
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
Minimálně 48x10/100/1000 RJ-45, 4x10GE SFP/SFP+	ANO	Minimálně 48x10/100/1000 RJ-45, 4x10GE SFP/SFP+
PoE budget až 740W a podpora 802.3aft/at na všech access RJ-45 portech	ANO	PoE budget až 740W a podpora 802.3aft/at na všech access RJ-45 portech
Samostatný konzolový port, L3 mgmt port a USB port	ANO	Samostatný konzolový port, L3 mgmt port (L3 mgmt port – Lze provést konfiguračně) a USB port
Velikost maximálně 1RU	ANO	Velikost 1RU
Minimální přepínací kapacita 170 Gbps	ANO	Minimální přepínací kapacita 170 Gbps
Propustnost minimálně 250 Mpps	ANO	Propustnost minimálně 250 Mpps
Velikost bufferu pro spracování paketů je alespoň 2MB per port	ANO	Velikost bufferu pro spracování paketů je alespoň 2MB per port
Minimální velikost MAC tabulky alespoň 32000 záznamů	ANO	Minimální velikost MAC tabulky alespoň 32000 záznamů
Minimální počet podporovaných VLAN alespoň 4000	ANO	Minimální počet podporovaných VLAN alespoň 4000
Požadavky na podporu přepínačů výrobcem	ANO/NE	Popis splnění požadavku
Nativní podpora HW výrobce s možností výměny vadného HW do třiceti dnů a to až pět let po ohlášení konce možnosti objednat nabízený přepínač	ANO	Nativní podpora HW výrobce s možností výměny vadného HW do třiceti dnů a to až pět let po ohlášení konce možnosti objednat nabízený přepínač
Podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 a možnost výměny vadného zařízení v režimu 8x5. Obojí po dobu 5 let.	ANO	Podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 a možnost

		výměny vadného zařízení v režimu 8x5. Obojí po dobu 5 let.

přepínače s 24 porty s PoE

přepínače s 24 porty s PoE		
Požadovaný počet : 3		
Název a výrobce	**Výrobce: FORTINET** **Název: FortiSwitch-124F-FPOE** **+ 5 Year FortiCare Premium Support**	
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
Minimálně 24x 10/100/1000 RJ-45 a 4x 1000/10000 SFP+	ANO	Minimálně 24x 10/100/1000 RJ-45 a 4x 1000/10000 SFP+
PoE budget až 370 a podpora 802.3aft/at na všech access RJ-45 portech	ANO	PoE budget až 370 a podpora 802.3aft/at na všech access RJ-45 portech
Samostatný konzolový port	ANO	Samostatný konzolový port
Velikost maximálně 1RU	ANO	Velikost maximálně 1RU
Minimální přepínací kapacita 120 Gbps	ANO	Minimální přepínací kapacita 120 Gbps
Propustnost minimálně 180 Mpps	ANO	Propustnost minimálně 180 Mpps
Minimální počet podporovaných VLAN alespoň 4000	ANO	Minimální počet podporovaných VLAN alespoň 4000
Napájecí zdroj a přívodní elektrický kabel pro CZ jsou součástí dodávky	ANO	Napájecí zdroj a přívodní elektrický kabel pro CZ jsou součástí dodávky
Proudění vzduchu ze strany do zadní částí přepínače	ANO	Proudění vzduchu ze strany do zadní částí přepínače
Bez nutnosti aktivního chlazení přepínače	ANO	Bez nutnosti aktivního chlazení přepínače
Podpora duálního firmwaru	ANO	Podpora duálního firmwaru
Podpora sFlow pro IPv4	ANO	Podpora sFlow pro IPv4
Integrovaný nástroj pro packet capture	ANO	Integrovaný nástroj pro packet capture
Požadavky na podporu přepínačů výrobcem	ANO/NE	Popis splnění požadavku
Nativní podpora HW výrobce s možností výměny vadného HW do třiceti dnů a to až pět let po ohlášení konce možnosti objednat nabízený přepínač	ANO	Nativní podpora HW výrobce s možností výměny vadného HW do třiceti dnů a to až pět let po ohlášení konce možnosti objednat nabízený přepínač

Podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 a možnost výměny vadného zařízení v režimu 8x5. Obojí po dobu 5 let.	ANO	Podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 a možnost výměny vadného zařízení v režimu 8x5. Obojí po dobu 5 let.

SFP pro poptávané přepínače		
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
Požadovaný počet: Pro propojení nových switchů – minimální počet 30 ks	ANO	Požadovaný počet: Pro propojení nových switchů – minimální počet 30 ks
10G SFP+ Transceiver kompatibilní s nabízenými přepínači	ANO	10G SFP+ Transceiver kompatibilní s nabízenými přepínači

implementace

Aktivní prvky core switch a POE switch		
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
fyzická montáž zařízení a propojení do stávající síťové infrastruktury	ANO	fyzická montáž zařízení a propojení do stávající síťové infrastruktury
upgrade firmware na aktuální stabilní verzi doporučenou výrobcem	ANO	upgrade firmware na aktuální stabilní verzi doporučenou výrobcem
analýza stavu topologie a současné konfigurace	ANO	analýza stavu topologie a současné konfigurace
akceptační testy a testovací provoz	ANO	akceptační testy a testovací provoz
školení administrátorů v rozsahu 2 hodin	ANO	školení administrátorů v rozsahu 2 hodin
dokumentace skutečného provedení	ANO	dokumentace skutečného provedení

WiFi přístupový bod

WiFi přístupový bod		
Požadovaný počet : **25**		
Název a výrobce		**Výrobce: FORTINET** **Název: FortiAP-231K+ 5 Year FortiCare Premium Support**
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
Požadavky na řízení a správu přístupových bodů		
Přístupové body musí být centrálně řízeny a spravovány řešením v podobě on-premise nástroje nebo cloud platformy	ANO	Přístupové body jsou centrálně řízeny a spravovány řešením v podobě on-premise nástroje nebo cloud platformy
Ideálně nástroj centrální správy umožňuje terminovat provoz SSID, v tunelovém režimu, s ohledem na možnou potřebu segmentace drátového a bezdrátového provozu	ANO	Ideálně nástroj centrální správy umožňuje terminovat provoz SSID, v tunelovém režimu, s ohledem na možnou potřebu segmentace drátového a bezdrátového provozu
On-premise varianta řešení centrální správy může být součástí jiného, v tomto projektu nabízeného, produktu stejného výrobce	ANO	On-premise varianta řešení centrální správy může být součástí jiného, v tomto projektu nabízeného, produktu stejného výrobce
řešení musí splňovat:		
automatická nebo manuální autorizace přístupových bodů na základě auto discovery mechanismu	ANO	automatická nebo manuální autorizace přístupových bodů na základě auto discovery mechanismu
jednotné management rozhraní, ze kterého lze spravovat přístupové body a případně i další produkty stejného výrobce	ANO	jednotné management rozhraní, ze kterého lze spravovat přístupové body a případně i další produkty stejného výrobce
jednotné management rozhraní pro správu bezdrátové sítě a bezpečnostních politik souvisejících s konkrétním SSID	ANO	jednotné management rozhraní pro správu bezdrátové sítě a bezpečnostních politik souvisejících s konkrétním SSID
jednotné management rozhraní pro zobrazení stavu všech přístupových bodů včetně jim přiřazených SSID, asociovaných klientů interferujících SSID včetně síly signálu interferujícího	ANO	jednotné management rozhraní pro zobrazení stavu všech přístupových bodů včetně jim přiřazených SSID, asociovaných klientů interferujících SSID včetně síly signálu interferujícího

SSID vůči konkrétnímu přístupovému bodu		SSID vůči konkrétnímu přístupovému bodu
možnost vyhledávání, v jednotném management rozhraní, konkrétních připojených zařízení nebo uživatel na základě minimálně následujících parametrů: IP adresa, MAC adres, uživatelské jméno	ANO	možnost vyhledávání, v jednotném management rozhraní, konkrétních připojených zařízení nebo uživatel na základě minimálně následujících parametrů: IP adresa, MAC adres, uživatelské jméno
možnost automatické aktualizace operačního sytému přístupového bude po jeho připojení do sítě	ANO	možnost automatické aktualizace operačního sytému přístupového bude po jeho připojení do sítě
možnost automaticky registrovat přístupový bude na servisní portál výrobce	ANO	možnost automaticky registrovat přístupový bude na servisní portál výrobce
možnost automatické karantény konkrétního uživatele z jednotného management rozhraní, která zamezí další možnosti připojení se uživatele k bezdrátové síti	ANO	možnost automatické karantény konkrétního uživatele z jednotného management rozhraní, která zamezí další možnosti připojení se uživatele k bezdrátové síti
možnost hromadného upgrade firmware z jednotného management rozhraní	ANO	možnost hromadného upgrade firmware z jednotného management rozhraní
Konkrétní technické požadavky na bezdrátový přístupový bod	ANO	Konkrétní technické požadavky na bezdrátový přístupový bod
Formát zařízení: indoor s interními anténami	ANO	Formát zařízení: indoor s interními anténami
Příslušenství k montáži na zeď/strop/T-Rail	ANO	Příslušenství k montáži na zeď/strop/T-Rail
Počet rádií: minimálně 3 pro přenos v pásmech 2,4, 5 a 6GHz	ANO	Počet rádií: minimálně 3 pro přenos v pásmech 2,4, 5 a 6GHz
Podpora kanálů o šířce 160MHz v 6GHz pásmu	ANO	Podpora kanálů o šířce 160MHz v 6GHz pásmu
Podpora BSS Coloring	ANO	Podpora BSS Coloring
Minimálně 2x2 MIMO	ANO	Minimálně 2x2 MIMO
Dedikované Bluetooth/ZigBee rádio pro lokalizační služby	ANO	Dedikované Bluetooth/ZigBee rádio pro lokalizační služby
Možnost provozu dvou rádií v pásmu 5GHz	ANO	Možnost provozu dvou rádií v pásmu 5GHz

Alespoň 1x 10/100/1000 a 1x 1x 100/1000/2500 Base-T RJ45 Base-T RJ45 uplink porty s možností sestavení LAG	ANO	Alespoň 1x 10/100/1000 a 1x 1x 100/1000/2500 Base-T RJ45 Base-T RJ45 uplink porty s možností sestavení LAG
1x USB port 3.0 a 1x konzolový port RJ45	ANO	1x USB port 3.0 a 1x konzolový port RJ45
Možnost souběžně provozovat až 16 SSID	ANO	Možnost souběžně provozovat až 16 SSID
Podpora Cellular Co-existence, TWT (Target Wake Time)	ANO	Podpora Cellular Co-existence, TWT (Target Wake Time)
Možnost spektrální analýzy přímo na AP	ANO	Možnost spektrální analýzy přímo na AP
Možnost zachytávání paketů na zařízení pro jejich analýzu	ANO	Možnost zachytávání paketů na zařízení pro jejich analýzu
Podpora napájení pomocí 802.3af	ANO	Podpora napájení pomocí 802.3af
Podpora všech následujících standardů - 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11w, 802.11ac, 802.11ax, 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az	ANO	Podpora všech následujících standardů - 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11w, 802.11ac, 802.11ax, 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az
Kensigton lock na samotném AP	ANO	Kensigton lock na samotném AP
Požadavky na výrobcem	**ANO/NE**	**Popis splnění požadavku**
Podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 a možnost výměny vadného zařízení v režimu 8x5. Obojí po dobu 5 let.	ANO	Podpora výrobce na HW, operační systém a řešení konfiguračních a systémových problémů v režimu 24/7 a možnost výměny vadného zařízení v režimu 8x5. Obojí po dobu 5 let.

implementace

WiFi přístupový bod		
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
Zapojení do centrálního managementu	ANO	Zapojení do centrálního managementu
upgrade firmware na aktuální stabilní verzi doporučenou výrobcem	ANO	upgrade firmware na aktuální stabilní verzi doporučenou výrobcem
analýza stavu topologie a současné konfigurace	ANO	analýza stavu topologie a současné konfigurace
akceptační testy a testovací provoz	ANO	akceptační testy a testovací provoz
školení administrátorů v rozsahu 2 hodin	ANO	školení administrátorů v rozsahu 2 hodin
dokumentace skutečného provedení	ANO	dokumentace skutečného provedení

NAC - Realizace nástroje pro řízení přístupu na síti

Cílem je, aby se k interní síti mohli připojit pouze autorizovaní uživatelé a zařízení, a aby se tak zamezilo nežádoucím připojením k síti. Cílem je zajistit co možná nejsnazší, ale dostatečně robustní, politikou řízený a prosazovaný přístup k síti a jejím zdrojům s ohledem na aktuální stav přistupujícího i již připojeného zařízení.
Centrálně definované politiky budou určovat způsob, typ, místo a rozsah přístupu pro konkrétní skupiny uživatelů a zařízení (případně v kombinaci). 802.1x politika bude řídit nejen přístup pro adekvátně ověřené skupiny uživatelů a kategorie zařízení, ale má být dalším stupněm kybernetické ochrany. Jejím sekundárním úkolem proto bude dohlížet momentální stav již připojených zařízení a bezprostředně reagovat na jeho nežádoucí změnu (např. vypnutí AV ochrany, nebo projev jiné hrozby).

NAC		
Název a výrobce	**Výrobce: FORTINET** **Název: FortiNAC Control and Application Extended-VM + FortiCare Premium Support**	
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
Virtuální appliance pro platformu VMWARE ESX, Microsoft Hyper-V, KVM (HW alternativa není poptávána)	ANO	Virtuální appliance pro platformu VMWARE ESX, Microsoft Hyper-V, KVM
Možnost instalace VM v prostředí AWS a Azure s podporou HA režimu, který kombinuje cloud a on-prem instance	ANO	Možnost instalace VM v prostředí AWS a Azure s podporou HA režimu, který kombinuje cloud a on-prem instance
Podpora distribuované architektury s centrálním správním prvkem a distribuovanými autentizačními branami	ANO	Podpora distribuované architektury s centrálním správním prvkem a distribuovanými autentizačními branami
Autentizační brány musí být nasazené mimo samotný datový tok (tzv. inline řešení není akceptovatelné)	ANO	Autentizační brány mohou být nasazené mimo samotný datový tok
Podpora HA v režimu active-passive se sdílením licencí mezi aktivním a pasivním prvkem	ANO	Podpora HA v režimu active-passive se sdílením licencí mezi aktivním a pasivním prvkem
Možnost nasazení v režimu L2 nebo L3 jak pro HA, tak i pro komunikaci se síťovými prvky	ANO	Možnost nasazení v režimu L2 nebo L3 jak pro HA, tak i pro komunikaci se síťovými prvky

Schopnost NAC řešení komunikovat se síťovými prvky, drátovými i bezdrátovými, jiných výrobců pomocí SNMP a CLI a vymáhat na nich definované bezpečnostní politiky bez nutnosti využití 802.1x nebo MAB	ANO	Schopnost NAC řešení komunikovat se síťovými prvky, drátovými i bezdrátovými, jiných výrobců pomocí SNMP a CLI a vymáhat na nich definované bezpečnostní politiky bez nutnosti využití 802.1x nebo MAB
Možnost instalace samostatného NAC řešení v podobě pouze enforcement brány bez nutnosti nákupu dalších prvků, jako například centrální management. Pokud je další prvek nutný, musí být součástí nabídky.	ANO	Možnost instalace samostatného NAC řešení v podobě pouze enforcement brány bez nutnosti nákupu dalších prvků, jako například centrální management. Pokud je další prvek nutný, musí být součástí nabídky.
Autentizační brána je schopna poskytnout DHCP a DNS služby pro zařízení, která je třeba registrovat do systému před jejich vpuštěním do produkční sítě	ANO	Autentizační brána je schopna poskytnout DHCP a DNS služby pro zařízení, která je třeba registrovat do systému před jejich vpuštěním do produkční sítě
Autentizační brána funguje sama o sobě jako Radius server pro autentizaci i accounting	ANO	Autentizační brána funguje sama o sobě jako Radius server pro autentizaci i accounting
Všechny požadované funkce pokrývá jeden typ licence a je možné dodatečně zvýšit počet licencí v systému	ANO	Všechny požadované funkce pokrývá jeden typ licence a je možné dodatečně zvýšit počet licencí v systému
Správa řešení pomocí zabezpečeného webového rozhraní, pomocí CLI protokolem SSH a možnost granulárního nastavení administrátorských oprávnění do úrovně spravovaných síťových zařízení a portů	ANO	Správa řešení pomocí zabezpečeného webového rozhraní, pomocí CLI protokolem SSH a možnost granulárního nastavení administrátorských oprávnění do úrovně spravovaných síťových zařízení a portů
POŽADAVKY NA KONTROLU PŘÍSTUPU DO SÍTĚ		
Autentizace a bezpečnostní kontrola endpointu před jeho připojením do sítě (nezávisle na způsobu připojení jako wired, wireless, VPN)	ANO	Autentizace a bezpečnostní kontrola endpointu před jeho připojením do sítě (nezávisle na způsobu připojení jako wired, wireless, VPN)

Možnost detailní profilace připojeného zařízení a klienta a to buď manuálně vytvořeným pravidlem nebo na základě jeho otisku, který je získán skenem sítě nebo komunikací s externím systémy a to bez nutnosti dodatečného licencování této funkcionality	ANO	Možnost detailní profilace připojeného zařízení a klienta a to buď manuálně vytvořeným pravidlem nebo na základě jeho otisku, který je získán skenem sítě nebo komunikací s externím systémy a to bez nutnosti dodatečného licencování této funkcionality
Podpora politik pro automatickou profilaci zařízení (minimálně na základě: SNMP, RADIUS, SYSLOG, DHCP, API, SSH, NMAP, DHCP fingerprinting, HTTP(s), IP range, telnet, expect scripty, vyhodnocení TCP/UDP portů, VENDOR OUI/MAC, WMI profil, pollování firewallu a vyhodnocování síťové komunikace, perl skripty) a to bez nutnosti dodatečného licencování této funkcionality	ANO	Podpora politik pro automatickou profilaci zařízení (minimálně na základě: SNMP, RADIUS, SYSLOG, DHCP, API, SSH, NMAP, DHCP fingerprinting, HTTP(s), IP range, telnet, expect scripty, vyhodnocení TCP/UDP portů, VENDOR OUI/MAC, WMI profil, pollování firewallu a vyhodnocování síťové komunikace, perl skripty) a to bez nutnosti dodatečného licencování této funkcionality
Periodická kontrola připojeného zařízení, zda odpovídá profilu, na základě kterého bylo zařízeno vpuštěno do sítě a možnost odpojit zařízení v případě, kdy nesplňuje podmínky původního profilu	ANO	Periodická kontrola připojeného zařízení, zda odpovídá profilu, na základě kterého bylo zařízeno vpuštěno do sítě a možnost odpojit zařízení v případě, kdy nesplňuje podmínky původního profilu
Podporované autentizační protokoly: min. MS-CHAP v2, PAP, EAP-MD5, EAP-PEAP, EAP-TLS, EAP-FAST, EAP-TTLS	ANO	Podporované autentizační protokoly: min. MS-CHAP v2, PAP, EAP-MD5, EAP-PEAP, EAP-TLS, EAP-FAST, EAP-TTLS
Po úspěšné autentizaci je možné definovat parametry konfigurace síťového portu nebo SSID, kde je autentizovaná entita připojená, pomocí standartních Radius atributů	ANO	Po úspěšné autentizaci je možné definovat parametry konfigurace síťového portu nebo SSID, kde je autentizovaná entita připojená, pomocí standartních Radius atributů

Po úspěšné autentizaci je možné na síťové zařízení, kde je klient připojen, instalovat z NAC brány konfiguraci, jako například ACL	ANO	Po úspěšné autentizaci je možné na síťové zařízení, kde je klient připojen, instalovat z NAC brány konfiguraci, jako například ACL
Podpora 802.1x	ANO	Podpora 802.1x
Podpora MAB autentizace	ANO	Podpora MAB autentizace
Podpora tvorby lokálních účtů a lokální autentizace	ANO	Podpora tvorby lokálních účtů a lokální autentizace
Podpora registrace koncových zařízení v NAC řešení před jejich fyzickým připojením do sítě	ANO	Podpora registrace koncových zařízení v NAC řešení před jejich fyzickým připojením do sítě
Podpora funkce RADIUS proxy	ANO	Podpora funkce RADIUS proxy
Možnost integrace se stávající CA (certifikační autorita)	ANO	Možnost integrace se stávající CA (certifikační autorita)
Podpora agentů pro operační systémy: Windows, MacOS, Linux (agent dodává detailní informace o počítači, informace o login/logout, umožňuji spouštění skriptů a zajišťuje notifikace pro uživatele) a licence pro tyto agenty je součástí dodané licence	ANO	Podpora agentů pro operační systémy: Windows, MacOS, Linux (agent dodává detailní informace o počítači, informace o login/logout, umožňuji spouštění skriptů a zajišťuje notifikace pro uživatele) a licence pro tyto agenty je součástí dodané licence
Podpora Integrace se stávajícím AD serverem pro autentizaci uživatelů pomocí LDAP	ANO	Podpora Integrace se stávajícím AD serverem pro autentizaci uživatelů pomocí LDAP
Podpora captive portál v rámci autentizační brány s plně editovatelným prostředí	ANO	Podpora captive portál v rámci autentizační brány s plně editovatelným prostředí
Minimálně 5 různých captive portálů	ANO	Minimálně 5 různých captive portálů
Podpora tzv. sponzorovaného přístupu pro autentizaci hostů a BYOD zařízení s možností zaslání přístupových údajů pomocí SMS a Email	ANO	Podpora tzv. sponzorovaného přístupu pro autentizaci hostů a BYOD zařízení s možností zaslání přístupových údajů pomocí SMS a Email
NAC řešení je schopné zablokovat konektivitu připojeného zařízení nebo změnit síťový segment na úrovni přístupové vrstvy v případě zjištění bezpečnostního incidentu	ANO	NAC řešení je schopné zablokovat konektivitu připojeného zařízení nebo změnit síťový segment na úrovni přístupové vrstvy v případě zjištění bezpečnostního incidentu

Podpora integrace s MDM nástroji jako Microsoft In-Tune a dále s OT/ioT nástroji Nozomi, Claroty	ANO	Podpora integrace s MDM nástroji jako Microsoft In-Tune a dále s OT/ioT nástroji Nozomi, Claroty
Podpora integrace s poptávaným NGFW a analytickým nástrojem nad provozem poptávaného NGFW	ANO	Podpora integrace s poptávaným NGFW a analytickým nástrojem nad provozem poptávaného NGFW
Podpora alespoň RSSO komunikace s NGFW	ANO	Podpora alespoň RSSO komunikace s NGFW
Administrátor má možnost manuálně, volbou v GUI, registrovat, zablokovat, smazat nebo i definovat nové zařízení a uživatele	ANO	Administrátor má možnost manuálně, volbou v GUI, registrovat, zablokovat, smazat nebo i definovat nové zařízení a uživatele
POŽADAVKY NA ENDPOINT COMPLIANCE		
Endpoint compliance se provádí před povolením přístupu do sítě na základě definovaného profilu nebo agenta na koncové stanici	ANO	Endpoint compliance se provádí před povolením přístupu do sítě na základě definovaného profilu nebo agenta na koncové stanici
Endpoint compliance je možné provádět periodicky (v době, kdy je počítač připojen do sítě)	ANO	Endpoint compliance je možné provádět periodicky (v době, kdy je počítač připojen do sítě)
Kontrola stavu AV na stanici	ANO	Kontrola stavu AV na stanici
Kontrola stavu registrů	ANO	Kontrola stavu registrů
Kontrola existence konkrétních souborů v lokálním filesystému	ANO	Kontrola existence konkrétních souborů v lokálním filesystému
Ověření domény	ANO	Ověření domény
Ověření certifikátu a jeho částí jako je vydavatel, expirace, common-name, …	ANO	Ověření certifikátu a jeho částí jako je vydavatel, expirace, common-name, …
Ověření verze a patch na úrovni operačního systému	ANO	Ověření verze a patch na úrovni operačního systému
Podpora sběru informací o instalovaných aplikacích na endpointech	ANO	Podpora sběru informací o instalovaných aplikacích na endpointech
Notifikace uživatele v případě nesplnění bezpečnostní kontroly, s využitím funkce captive portál	ANO	Notifikace uživatele v případě nesplnění bezpečnostní kontroly, s využitím funkce captive portál

Možnost kontaktovat koncovou stanice v reálném čase textovou správu v případě nasazení endpoint agenta pro compliance	ANO	Možnost kontaktovat koncovou stanice v reálném čase textovou správu v případě nasazení endpoint agenta pro compliance
REPORTING		
Možnost tvorby reportů o stavu platformy a stavu připojených zařízení v reálném čase a alespoň zpětně o jeden týden. Reporting je nativní funkce dostupná v GUI bez nutnosti dodatečného licencování	ANO	Možnost tvorby reportů o stavu platformy a stavu připojených zařízení v reálném čase a alespoň zpětně o jeden týden. Reporting je nativní funkce dostupná v GUI bez nutnosti dodatečného licencování
NOTIFIKACE ADMINISTRÁTORŮ A UŽIVATELŮ	ANO	
Možnost napojení autentizační brány na SMS nebo email bránu promocí konektoru přímo z GUI	ANO	Možnost napojení autentizační brány na SMS nebo email bránu promocí konektoru přímo z GUI
POŽADAVKY NA LICENCE A PODPORU VÝROBCE		
Licence pro min. 1500 endpointů	ANO	Licence pro min. 1500 endpointů
Podpora výrobce v režimu 24x7 pro platformu i její provozní konfiguraci včetně politik na 5 let	ANO	Podpora výrobce v režimu 24x7 pro platformu i její provozní konfiguraci včetně politik na 5 let

implementace

NAC		
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
analýza stavu topologie a současné konfigurace	ANO	analýza stavu topologie a současné konfigurace
akceptační testy a testovací provoz	ANO	akceptační testy a testovací provoz
školení administrátorů v rozsahu 2 hodin	ANO	školení administrátorů v rozsahu 2 hodin
dokumentace skutečného provedení	ANO	dokumentace skutečného provedení

Analýza a ukládání logů

Analýza a ukládání logů		
Název a výrobce	**Výrobce: FORTINET** **Název: FortiAnalyzer-VM Subscription License with Support**	
základní technické požadavky	ANO/NE	Popis splnění požadavku
nástroj pro bezpečnostní analýzu logů z NGFW zařízení se schopností jejich korelace včetně možnosti ukládání logů	ANO	nástroj pro bezpečnostní analýzu logů z NGFW zařízení se schopností jejich korelace včetně možnosti ukládání logů
podpora automatizace reakcí na bezpečnostní události detekované nabízeným řešením směrem k NGFW zařízení přímo v grafickém rozhraní nabízeného řešení	ANO	podpora automatizace reakcí na bezpečnostní události detekované nabízeným řešením směrem k NGFW zařízení přímo v grafickém rozhraní nabízeného řešení
virtuální appliance pro platformu VMWare, Microsoft Hyper-V, KVM (fyzické zařízení není přípustná alternativa)	ANO	virtuální appliance pro platformu VMWare, Microsoft Hyper-V, KVM (fyzické zařízení není přípustná alternativa)
možnost nativní integrace s poptávaným zařízením typu NGFW, které bude sloužit jako zdroj dat pro analýzu	ANO	možnost nativní integrace s poptávaným zařízením typu NGFW, které bude sloužit jako zdroj dat pro analýzu
alespoň 5TB alokovatelná kapacita dlouhodobého úložiště logů a alespoň 5GB minimální limit pro množství přijatých logů k analýze za jeden den (možnost navýšení limitů pomocí dodatečné licence)	ANO	alespoň 5TB alokovatelná kapacita dlouhodobého úložiště logů a alespoň 5GB minimální limit pro množství přijatých logů k analýze za jeden den (možnost navýšení limitů pomocí dodatečné licence)
minimálně 4x vNIC	ANO	minimálně 4x vNIC
možnost provozovat poptávané řešení jako prosté uložiště logů z dalších zařízení zákazníka bez jejich další analýzy	ANO	možnost provozovat poptávané řešení jako prosté uložiště logů z dalších zařízení zákazníka bez jejich další analýzy
možnost tvorby komplexních reportů (Top X uživatelů/zařízení dle množství zjištěných hrozeb, přeneseného provozu atd.) nad analyzovanými daty z grafického rozhraní poptávaného nástroje	ANO	možnost tvorby komplexních reportů (Top X uživatelů/zařízení dle množství zjištěných hrozeb, přeneseného provozu atd.) nad analyzovanými daty z grafického rozhraní poptávaného nástroje
možnost generovat reporty na základě specifikace dotazů do databáze logů poptávaného řešení	ANO	možnost generovat reporty na základě specifikace dotazů do databáze logů poptávaného řešení

HTML/CSV/XML/PDF formát generovaných reportů s možností plánování pravidelné automatické tvorby reportů	ANO	HTML/CSV/XML/PDF formát generovaných reportů s možností plánování pravidelné automatické tvorby reportů
možnost logické segmentace s možností izolace jednotlivých segmentů z hlediska jejich administrace a zdroje dat	ANO	možnost logické segmentace s možností izolace jednotlivých segmentů z hlediska jejich administrace a zdroje dat
musí obsahovat předdefinované vzory reportů a umožňovat úpravu vzhledu generovaných reportů prvky zákazníka (loga, hlavička, …)	ANO	obsahuje předdefinované vzory reportů a umožňovat úpravu vzhledu generovaných reportů prvky zákazníka (loga, hlavička, …)
možnost zobrazení aktuálních logů z jednotlivých integrovaných NGFW zařízení v reálném čase	ANO	možnost zobrazení aktuálních logů z jednotlivých integrovaných NGFW zařízení v reálném čase
možnost zpětného zobrazení a analýzy logů z důvodu možnosti zpětné analýzy provozu a možných uskutečněných bezpečnostních hrozeb	ANO	možnost zpětného zobrazení a analýzy logů z důvodu možnosti zpětné analýzy provozu a možných uskutečněných bezpečnostních hrozeb
požadavky na management	ANO/NE	Popis splnění požadavku
plnohodnotná správa pomocí grafického rozhraní a CLI	ANO	plnohodnotná správa pomocí grafického rozhraní a CLI
podpora SNMPv2 a SNMPv3 a REST API	ANO	podpora SNMPv2 a SNMPv3 a REST API
samostatná sekce v grafickém rozhraní pro zobrazení zjištěných hrozeb	ANO	FortiView Threats
podpora přijímání syslogů ze zařízení třetích stran	ANO	podpora přijímání syslogů ze zařízení třetích stran
možnost šifrování přenášené komunikace mezi poptávaným řešením pro analýzu dat a poptávaným NGFW zařízením	ANO	možnost šifrování přenášené komunikace mezi poptávaným řešením pro analýzu dat a poptávaným NGFW zařízením
další požadavky	ANO/NE	Popis splnění požadavku
podpora výrobce v režimu 24/7 na dobu min. 5 let	ANO	podpora výrobce v režimu 24/7 na dobu min. 5 let
všechny potřebné licence pro výše uvedené funkce a minimální parametry na dobu min. 5 let musí být také součástí dodávky	ANO	všechny potřebné licence pro výše uvedené funkce a minimální parametry na dobu min. 5 let musí být také součástí dodávky

implementace

Analýza a ukládání logů- implementace		
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
instalace zařízení a propojení do stávající síťové infrastruktury	ANO	instalace zařízení a propojení do stávající síťové infrastruktury
upgrade firmware na aktuální stabilní verzi doporučenou výrobcem	ANO	upgrade firmware na aktuální stabilní verzi doporučenou výrobcem
analýza stavu topologie a současné konfigurace	ANO	analýza stavu topologie a současné konfigurace
akceptační testy a testovací provoz	ANO	akceptační testy a testovací provoz
implementace management nástroje a napojení všech prvků do managementu	ANO	implementace management nástroje a napojení všech prvků do managementu
implementace nástroje pro bezpečnostní analýzu logů z NGFW zařízení se schopnosti jejich korelace včetně možnosti ukládání logů	ANO	implementace nástroje pro bezpečnostní analýzu logů z NGFW zařízení se schopnosti jejich korelace včetně možnosti ukládání logů

ID002 - Zvýšení redundance a zabezpečení primárního datového centra

IS je díky tomu možno provozovat ve vysoké dostupnosti a rovněž jej velmi efektivně zálohovat. Jedná se klíčový IS školy, který naplňuje potřeby žáků v rámci doplňujících služeb školy

Specifikace aplikačního serveru

Nabízený výrobek plní všechny požadované parametry.

Specifikace aplikačního serveru		
Název a výrobce	**Výrobce DELL** **Název: SERVER DELL PowerEdge R760 – konfigurace plnící všechny min. tech specifikace**	
Požadovaný počet : 2		
Technický parametr	Minimální technické požadavky	Popis splnění požadavku
Form Factor a vnitřní uspořádání	2U, pro přístup ke všem komponentám serveru není nutné nářadí, barevně značené hot-plug vnitřní komponenty a místa pro uchopení. Uzamykatelný přední panel.	2U, pro přístup ke všem komponentám serveru není nutné nářadí, barevně značené hot-plug vnitřní komponenty a místa pro uchopení. Uzamykatelný přední panel.
CPU	Dvousocketový systém založený na Intel platformě s využitím páté generace CPU Xeon. / AMD	Dvousocketový systém založený na Intel platformě s využitím páté generace CPU Xeon. / AMD
	Osazený 2x CPU s 8mi jádry, o základní frekvenci min. 2.6 GHz. Celkový výkon musí dosahovat minimálně 41400 bodů dle https://www.cpubenchmark.net	Osazený 2x CPU s 8mi jádry, o základní frekvenci min. 2.6 GHz. Celkový výkon dosahuje minimálně 41400 bodů dle https://www.cpubenchmark.net
RAM	8x 32GB na 5600MHz s možností osazení až 32 slotů.	8x 32GB na 5600MHz s možností osazení až 32 slotů.
Diskový subsystém	Server musí podporovat osazení min. 12x 3,5 palcových disků typu SAS/SATA, požadujeme server disky:	Server podporuje osazení min. 12x 3,5 palcových disků typu SAS/SATA, server disky:
	Vlastní bootovací karta pro instalaci hypervizoru osazená minimálně:	Vlastní bootovací karta pro instalaci hypervizoru osazená minimálně:
	· 2x 480GB M.2 SSD NVMe v RAID1	· 2x 480GB M.2 SSD NVMe v RAID1

Diskový řadič	· typu SAS, PCI Express 4 kompatibilní, dvoukanálový (2 konektory)	· typu SAS, PCI Express 4 kompatibilní, dvoukanálový (2 konektory)
	· podpora RAID 0, 1, 5, 6, 10, 50, 60	· podpora RAID 0, 1, 5, 6, 10, 50, 60
	· podpora 12Gbps technologie rozhraní disků	· podpora 12Gbps technologie rozhraní disků
	· podpora Capacity Expansion (OCE)	· podpora Capacity Expansion (OCE)
	· podpora RAID Level Migration (RLM)	· podpora RAID Level Migration (RLM)
	· podpora SED disků a SSD disků	· podpora SED disků a SSD disků
Síťové rozhraní	1 x 1GbE port Base-T (RJ45) Dual Port	1 x 1GbE port Base-T (RJ45) Dual Port
	1 x 10/25 GbE port Ethernet typu SFP28 Dual Port	1 x 10/25 GbE port Ethernet typu SFP28 Dual Port
	1 x 10 GbE port typu Base-T (RJ45) Dual Port	1 x 10 GbE port typu Base-T (RJ45) Dual Port
Napájení	Plně redundantní síťové napájecí zdroje 1100W s možností nastavení limitů výkonu a spotřeby v BIOSu (Power Budgeting) 96% účinnost při zatížení 50% (Titanium)	Plně redundantní síťové napájecí zdroje 1100W s možností nastavení limitů výkonu a spotřeby v BIOSu (Power Budgeting) 96% účinnost při zatížení 50% (Titanium)
Interface	· 3 x USB (1 vpředu, 2 vzadu), min. 1x USB 3.0	· 3 x USB (1 vpředu, 2 vzadu), min. 1x USB 3.0
	· 2 x VGA (1 vpředu, 1 vzadu)	· 2 x VGA (1 vpředu, 1 vzadu)
Rozšiřující sloty	· Min 3x PCIe Gen4/5 sloty volné pro budoucí použití	· Min 3x PCIe Gen4/5 sloty volné pro budoucí použití
Kolejnice	· Zásuvné ližiny s ramenem pro vedení kabelů	· Zásuvné ližiny s ramenem pro vedení kabelů
Kompatibilita	· Microsoft® Windows Server® 2019/2022, x64	· Microsoft® Windows Server® 2019/2022, x64
	· SUSE® Linux® Enterprise Server	· SUSE® Linux® Enterprise Server
	· Red Hat® Enterprise Linux	· Red Hat® Enterprise Linux

	· Canonical Ubuntu Server LTS	· Canonical Ubuntu Server LTS
	· VMware vSphere™	· VMware vSphere™
Operační systém	· Windows Datacenter 2022 – licence na všechna jádra	· Windows Datacenter 2022 – licence na všechna jádra
Management a vzdálená správa	· samostatný dedikovaný LAN RJ45 port, který se nezapočítává do konektivity serveru	· samostatný dedikovaný LAN RJ45 port, který se nezapočítává do konektivity serveru
	· s podporou failoveru na jinou síťovou kartu v serveru, musí podporovat VLAN a LLDP Discovery síťové infrastruktury, protokolů IPv4 a IPv6	· s podporou failoveru na jinou síťovou kartu v serveru, musí podporovat VLAN a LLDP Discovery síťové infrastruktury, protokolů IPv4 a IPv6
	· monitoring jakékoliv komponenty serveru nesmí vyžadovat instalaci agenta do OS, OS se musí kompletně obejít bez AMS (Agentless Management Service). Tento požadavek se týká i diskového systému, včetně přístupu k nastavení RAID řadičů, SAS HBA či případných expansních diskových polic serveru. V případě síťových karet na desce či mezzanine kartě, musí být v managementu možnost monitorování až do úrovně případných optický modulů (SFP) osazených v těchto kartách	· monitoring jakékoliv komponenty serveru nnevyžaduje instalaci agenta do OS, OS se musí kompletně obejít bez AMS (Agentless Management Service). Tento požadavek se týká i diskového systému, včetně přístupu k nastavení RAID řadičů, SAS HBA či případných expansních diskových polic serveru. V případě síťových karet na desce či mezzanine kartě, je v managementu možnost monitorování až do úrovně případných optický modulů (SFP) osazených v těchto kartách
	· vestavěný HTML5 server pro správu bez nutnosti instalace ActiveX nebo Java pluginů, platí i pro vzdálenou konzoli KVM over IP	· vestavěný HTML5 server pro správu bez nutnosti instalace ActiveX nebo Java pluginů, platí i pro vzdálenou konzoli KVM over IP
	· management musí průběžně vyhodnocovat průměrné vytížení serveru s grafickým zobrazením v HTML5 GUI a možností alertů v případě excesů	· management průběžně vyhodnocuje průměrné vytížení serveru s grafickým zobrazením v HTML5 GUI a možností alertů v případě excesů

	· automatická instalace a obnova SSL certifikátu vestavěného serveru	· automatická instalace a obnova SSL certifikátu vestavěného serveru
	· přístup po SSL, Telnetu, SNMP a RESTful API s podporou Redfish SSE	· přístup po SSL, Telnetu, SNMP a RESTful API s podporou Redfish SSE
	· podpora multifaktorové autentizace, podpora MS AD a generického LDAP	· podpora multifaktorové autentizace, podpora MS AD a generického LDAP
	· možnost streamingu údajů senzorů serveru, telemetrie a reportů o provozu pro účely prediktivního vyhodnocování provozu a zabezpečení s podporou pro Splunk nebo ELK stack	· možnost streamingu údajů senzorů serveru, telemetrie a reportů o provozu pro účely prediktivního vyhodnocování provozu a zabezpečení s podporou pro Splunk nebo ELK stack
	· data logů musí být možné přesměrovat na sériový port RS232. Podpora Syslog serveru. Logy zaznamenávají stavy hardwarových sensorů (stav, teplota, napětí, …) včetně událostí o přihlášení a změnách konfigurace	· data logů je možné přesměrovat na sériový port RS232. Podpora Syslog serveru. Logy zaznamenávají stavy hardwarových sensorů (stav, teplota, napětí, …) včetně událostí o přihlášení a změnách konfigurace
	· podpora uzamčení stavu serveru pro zvýšení bezpečnosti (System Lock Down), automatický Secure OS recovery včetně BIOS serveru a firmware BMC, firmware rollback	· podpora uzamčení stavu serveru pro zvýšení bezpečnosti (System Lock Down), automatický Secure OS recovery včetně BIOS serveru a firmware BMC, firmware rollback
	· podpora dynamických změn nastavení externích USB portů systému, pro vzdálené povolení či zakázání portů, bez nutnosti restartu serveru či managementu	· podpora dynamických změn nastavení externích USB portů systému, pro vzdálené povolení či zakázání portů, bez nutnosti restartu serveru či managementu
	· podpora serverových konfiguračních profilů pro kompletně automatický deployment serverů vzdáleně i lokálně (Zero Touch deployment)	· podpora serverových konfiguračních profilů pro kompletně automatický deployment serverů vzdáleně i lokálně (Zero Touch deployment)

	· management musí umět poskytovat ovladače instalovaným operačním systémům bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS) a hardware firmware update s možností ověření a stažení aktuálních verzí proti online repository výrobce, případně zabezpečenému lokálnímu repository pod správou administrátora	· management musí umět poskytovat ovladače instalovaným operačním systémům bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS) a hardware firmware update s možností ověření a stažení aktuálních verzí proti online repository výrobce, případně zabezpečenému lokálnímu repository pod správou administrátora
	· management musí umět poskytovat FW zařízením a kartám instalovaných v serveru, s možností automatické obnovy používané verze a konfigurace v případě výměny zařízení / karty z důvodu servisního zásahu, včetně konfigurace biosu a samotného managementu. Vzdálený mount úložiště není dostatečný, z důvodu případné nízké propustnosti správcova připojení.	· management musí umět poskytovat FW zařízením a kartám instalovaných v serveru, s možností automatické obnovy používané verze a konfigurace v případě výměny zařízení / karty z důvodu servisního zásahu, včetně konfigurace biosu a samotného managementu. Vzdálený mount úložiště není dostatečný, z důvodu případné nízké propustnosti správcova připojení.

	· OOB karta serveru musí být schopna utvořit management skupinu s dalšími servery, tak aby prostředí mohlo být dohlíženo z jedné IP adresy bez nutnosti instalace externí management aplikace. Databáze takové skupiny musí být minimálně na dvou místech tak aby v případě výpadku jedné OOB karty, převzala funkcionalitu druhá v jiném serveru. Funkcionalita musí být alespoň v režimu master-slave (či active-pasive) a podporovat min. 100 serverů ve skupině	· OOB karta serveru je schopna utvořit management skupinu s dalšími servery, tak aby prostředí mohlo být dohlíženo z jedné IP adresy bez nutnosti instalace externí management aplikace. Databáze takové skupiny musí být minimálně na dvou místech tak aby v případě výpadku jedné OOB karty, převzala funkcionalitu druhá v jiném serveru. Funkcionalita musí být alespoň v režimu master-slave (či active-pasive) a podporovat min. 100 serverů ve skupině
	· OOB karta musí mít vestavěnu funkcionalitu automatického odeslání hrozících či vzniklých chybových stavů na helpdesk výrobce serverů a automatického vytvoření servisního incidentu, na základě, kterého se automaticky rozběhne servisní zásah (call-home)	· OOB karta musí mít vestavěnu funkcionalitu automatického odeslání hrozících či vzniklých chybových stavů na helpdesk výrobce serverů a automatického vytvoření servisního incidentu, na základě, kterého se automaticky rozběhne servisní zásah (call-home)
	· možnost přístupu přes dedikovaný USB port s emulací síťového připojení	· možnost přístupu přes dedikovaný USB port s emulací síťového připojení
	· vzdálený reset, reboot s korektním ukončením OS, vypnutí a zapnutí serveru, včetně odpojení zdrojů (power cycle)	· vzdálený reset, reboot s korektním ukončením OS, vypnutí a zapnutí serveru, včetně odpojení zdrojů (power cycle)
	· management musí umožnit bezpečné smazání dat ze serveru a jeho médií pro případ vyřazení nebo přesunu serveru	· management musí umožnit bezpečné smazání dat ze serveru a jeho médií pro případ vyřazení nebo přesunu serveru

	· licence OOB managementu musí být pro server trvalá (life time), pokud je vyžadována. Výrobce udržuje databázi zakoupených licencí přístupnou kupujícímu, tak aby ji bylo možné v případě výměny HW kdykoliv obnovit, pokud dojte ke ztrátě	· licence OOB managementu je pro server trvalá (life time), pokud je vyžadována. Výrobce udržuje databázi zakoupených licencí přístupnou kupujícímu, tak aby ji bylo možné v případě výměny HW kdykoliv obnovit, pokud dojte ke ztrátě
	· management umožňuje monitoring spotřeby el. energie na úrovni serveru	· management umožňuje monitoring spotřeby el. energie na úrovni serveru
	· identifikace připojeného vzdáleného uživatele	· identifikace připojeného vzdáleného uživatele
	· vzdálená identifikace serveru	· vzdálená identifikace serveru
Bezpečnostní funkce	· Server musí být doručen s jedinečným HASH klíčem, který ověří neměnnost HW a SW komponent po celou dobu dopravního procesu z továrny výrobce až ke koncovému uživateli	· Server je doručen s jedinečným HASH klíčem, který ověří neměnnost HW a SW komponent po celou dobu dopravního procesu z továrny výrobce až ke koncovému uživateli
Podpora a servis	· Technická podpora a servis na 5 let (24x7x365), jediné kontaktní místo pro hlášení poruch pro všechny HW i SW komponenty dodávaného systému od výrobce. Technická podpora a servis je poskytován výrobcem HW. Zahájení servisních prací následující pracovní den od identifikace problému. Servis probíhá v místě instalace HW. Zdarma možnost stažení ovladačů a Firmware ze stránek výrobce pro konkrétní HW, po zadání jedinečného identifikátoru. Tato možnost stažení ovladačů a Firmware není omezena na dobu trvání technické podpory.	· Technická podpora a servis na 5 let (24x7x365), jediné kontaktní místo pro hlášení poruch pro všechny HW i SW komponenty dodávaného systému od výrobce. Technická podpora a servis je poskytován výrobcem HW. Zahájení servisních prací následující pracovní den od identifikace problému. Servis probíhá v místě instalace HW. Zdarma možnost stažení ovladačů a Firmware ze stránek výrobce pro konkrétní HW, po zadání jedinečného identifikátoru. Tato možnost stažení ovladačů a Firmware není omezena na dobu trvání technické podpory.

	· Zdarma přístup k aktualizacím firmware a ovladačů i po uplynutí doby platné podpory.	· Zdarma přístup k aktualizacím firmware a ovladačů i po uplynutí doby platné podpory.
	Prodávající se zavazuje, že zařízení a veškeré jeho komponenty:	Prodávající se zavazuje, že zařízení a veškeré jeho komponenty:
	· pochází z autorizovaného obchodního kanálu výrobce	· pochází z autorizovaného obchodního kanálu výrobce
	· je licencováno ve jménu kupujícího, včetně příslušného softwarového vybavení	· je licencováno ve jménu kupujícího, včetně příslušného softwarového vybavení
	· je reportováno zpět výrobci a kupující je uveden v databázi výrobce jako konečný uživatel	· je reportováno zpět výrobci a kupující je uveden v databázi výrobce jako konečný uživatel

SERVER BACKUP

Nabízený výrobek plní všechny požadované parametry.

SERVER BACKUP		
Název a výrobce	**Výrobce DELL** **Název: SERVER DELL PowerEdge R760 – konfigurace plnící všechny min. tech specifikace**	
Požadovaný počet : 1		
Technický parametr	Minimální technické požadavky	Popis splnění požadavku
Form Factor a vnitřní uspořádání	2U, pro přístup ke všem komponentám serveru není nutné nářadí, barevně značené hot-plug vnitřní komponenty a místa pro uchopení. Uzamykatelný přední panel.	2U, pro přístup ke všem komponentám serveru není nutné nářadí, barevně značené hot-plug vnitřní komponenty a místa pro uchopení. Uzamykatelný přední panel.
CPU	Dvousocketový systém založený na Intel platformě s využitím páté generace CPU Xeon. /AMD	Dvousocketový systém založený na Intel platformě s využitím páté generace CPU Xeon. /AMD
	Osazený 2x CPU s 8mi jádry, o základní frekvenci min. 2.6 GHz. Celkový výkon musí dosahovat minimálně 41400 bodů dle https://www.cpubenchmark.net	Osazený 2x CPU s 8mi jádry, o základní frekvenci min. 2.6 GHz. Celkový výkon dosahuje minimálně 41400 bodů dle https://www.cpubenchmark.net
RAM	8x 32GB na 5600MHz s možností osazení až 32 slotů.	8x 32GB na 5600MHz s možností osazení až 32 slotů.
Diskový subsystém	Server musí podporovat osazení min. 12x 3,5 palcových disků typu SAS/SATA, požadujeme server osazený hot-plug disky:	Server podporuje osazení min. 12x 3,5 palcových disků typu SAS/SATA, server osazený hot-plug disky:
	3x 12TB 7.2K RPM SATA 6Gbps 512e 3.5in Hot-plug Hard Drive	4x 12TB 7.2K RPM SATA 6Gbps 512e 3.5in Hot-plug Hard Drive
	Vlastní bootovací karta pro instalaci hypervizoru osazená minimálně:	Vlastní bootovací karta pro instalaci hypervizoru osazená minimálně:
	· 2x 480GB M.2 SSD NVMe v RAID1	· 2x 480GB M.2 SSD NVMe v RAID1

Diskový řadič	· typu SAS, PCI Express 4 kompatibilní, dvoukanálový (2 konektory)	· typu SAS, PCI Express 4 kompatibilní, dvoukanálový (2 konektory)
	· podpora RAID 0, 1, 5, 6, 10, 50, 60	· podpora RAID 0, 1, 5, 6, 10, 50, 60
	· podpora 12Gbps technologie rozhraní disků	· podpora 12Gbps technologie rozhraní disků
	· podpora Capacity Expansion (OCE)	· podpora Capacity Expansion (OCE)
	· podpora RAID Level Migration (RLM)	· podpora RAID Level Migration (RLM)
	· podpora SED disků a SSD disků	· podpora SED disků a SSD disků
Síťové rozhraní	1 x 1GbE port Base-T (RJ45) Dual Port	1 x 1GbE port Base-T (RJ45)
	1 x 10/25 GbE port Ethernet typu SFP28 Dual Port	1 x 10/25 GbE port Ethernet typu SFP28
	1 x 10 GbE port typu Base-T (RJ45) Dual Port	1 x 10 GbE port typu Base-T (RJ45)
Napájení	Plně redundantní síťové napájecí zdroje 1100W s možností nastavení limitů výkonu a spotřeby v BIOSu (Power Budgeting) 96% účinnost při zatížení 50% (Titanium)	Plně redundantní síťové napájecí zdroje 1100W s možností nastavení limitů výkonu a spotřeby v BIOSu (Power Budgeting) 96% účinnost při zatížení 50% (Titanium)
Interface	· 3 x USB (1 vpředu, 2 vzadu), min. 1x USB 3.0	· 3 x USB (1 vpředu, 2 vzadu), min. 1x USB 3.0
	· 2 x VGA (1 vpředu, 1 vzadu)	· 2 x VGA (1 vpředu, 1 vzadu)
Rozšiřující sloty	· Min 3x PCIe Gen4/5 sloty volné pro budoucí použití	· Min 3x PCIe Gen4/5 sloty volné pro budoucí použití
Kolejnice	· Zásuvné ližiny s ramenem pro vedení kabelů	· Zásuvné ližiny s ramenem pro vedení kabelů
Kompatibilita	· Microsoft® Windows Server® 2019/2022, x64	· Microsoft® Windows Server® 2019/2022, x64
	· SUSE® Linux® Enterprise Server	· SUSE® Linux® Enterprise Server
	· Red Hat® Enterprise Linux	· Red Hat® Enterprise Linux

	· Canonical Ubuntu Server LTS	· Canonical Ubuntu Server LTS
	· VMware vSphere™	· VMware vSphere™
Operační systém	· Windows Datacenter 2022 – licence na všechna jádra	· Windows Datacenter 2022 – licence na všechna jádra
Management a vzdálená správa	· samostatný dedikovaný LAN RJ45 port, který se nezapočítává do konektivity serveru	· samostatný dedikovaný LAN RJ45 port, který se nezapočítává do konektivity serveru
	· s podporou failoveru na jinou síťovou kartu v serveru, musí podporovat VLAN a LLDP Discovery síťové infrastruktury, protokolů IPv4 a IPv6	· s podporou failoveru na jinou síťovou kartu v serveru, musí podporovat VLAN a LLDP Discovery síťové infrastruktury, protokolů IPv4 a IPv6
	· monitoring jakékoliv komponenty serveru nesmí vyžadovat instalaci agenta do OS, OS se musí kompletně obejít bez AMS (Agentless Management Service). Tento požadavek se týká i diskového systému, včetně přístupu k nastavení RAID řadičů, SAS HBA či případných expansních diskových polic serveru. V případě síťových karet na desce či mezzanine kartě, musí být v managementu možnost monitorování až do úrovně případných optický modulů (SFP) osazených v těchto kartách	· monitoring jakékoliv komponenty serveru nevyžaduje instalaci agenta do OS, OS se obejde bez AMS (Agentless Management Service). Tento požadavek se týká i diskového systému, včetně přístupu k nastavení RAID řadičů, SAS HBA či případných expansních diskových polic serveru. V případě síťových karet na desce či mezzanine kartě, musí být v managementu možnost monitorování až do úrovně případných optický modulů (SFP) osazených v těchto kartách
	· vestavěný HTML5 server pro správu bez nutnosti instalace ActiveX nebo Java pluginů, platí i pro vzdálenou konzoli KVM over IP	· vestavěný HTML5 server pro správu bez nutnosti instalace ActiveX nebo Java pluginů, platí i pro vzdálenou konzoli KVM over IP

	· management musí průběžně vyhodnocovat průměrné vytížení serveru s grafickým zobrazením v HTML5 GUI a možností alertů v případě excesů	· management průběžně vyhodnocuje průměrné vytížení serveru s grafickým zobrazením v HTML5 GUI a možností alertů v případě excesů
	· automatická instalace a obnova SSL certifikátu vestavěného serveru	· automatická instalace a obnova SSL certifikátu vestavěného serveru
	· přístup po SSL, Telnetu, SNMP a RESTful API s podporou Redfish SSE	· přístup po SSL, Telnetu, SNMP a RESTful API s podporou Redfish SSE
	· podpora multifaktorové autentizace, podpora MS AD a generického LDAP	· podpora multifaktorové autentizace, podpora MS AD a generického LDAP
	· možnost streamingu údajů senzorů serveru, telemetrie a reportů o provozu pro účely prediktivního vyhodnocování provozu a zabezpečení s podporou pro Splunk nebo ELK stack	· možnost streamingu údajů senzorů serveru, telemetrie a reportů o provozu pro účely prediktivního vyhodnocování provozu a zabezpečení s podporou pro Splunk nebo ELK stack
	· data logů musí být možné přesměrovat na sériový port RS232. Podpora Syslog serveru. Logy zaznamenávají stavy hardwarových sensorů (stav, teplota, napětí, …) včetně událostí o přihlášení a změnách konfigurace	· data logů je možné přesměrovat na sériový port RS232. Podpora Syslog serveru. Logy zaznamenávají stavy hardwarových sensorů (stav, teplota, napětí, …) včetně událostí o přihlášení a změnách konfigurace
	· podpora uzamčení stavu serveru pro zvýšení bezpečnosti (System Lock Down), automatický Secure OS recovery včetně BIOS serveru a firmware BMC, firmware rollback	· podpora uzamčení stavu serveru pro zvýšení bezpečnosti (System Lock Down), automatický Secure OS recovery včetně BIOS serveru a firmware BMC, firmware rollback

	· podpora dynamických změn nastavení externích USB portů systému, pro vzdálené povolení či zakázání portů, bez nutnosti restartu serveru či managementu	· podpora dynamických změn nastavení externích USB portů systému, pro vzdálené povolení či zakázání portů, bez nutnosti restartu serveru či managementu
	· podpora serverových konfiguračních profilů pro kompletně automatický deployment serverů vzdáleně i lokálně (Zero Touch deployment)	· podpora serverových konfiguračních profilů pro kompletně automatický deployment serverů vzdáleně i lokálně (Zero Touch deployment)
	· management musí umět poskytovat ovladače instalovaným operačním systémům bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS) a hardware firmware update s možností ověření a stažení aktuálních verzí proti online repository výrobce, případně zabezpečenému lokálnímu repository pod správou administrátora	· management umí poskytovat ovladače instalovaným operačním systémům bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS) a hardware firmware update s možností ověření a stažení aktuálních verzí proti online repository výrobce, případně zabezpečenému lokálnímu repository pod správou administrátora
	· management musí umět poskytovat FW zařízením a kartám instalovaných v serveru, s možností automatické obnovy používané verze a konfigurace v případě výměny zařízení / karty z důvodu servisního zásahu, včetně konfigurace biosu a samotného managementu. Vzdálený mount úložiště není dostatečný, z důvodu případné nízké propustnosti správcova připojení.	· management umí poskytovat FW zařízením a kartám instalovaných v serveru, s možností automatické obnovy používané verze a konfigurace v případě výměny zařízení / karty z důvodu servisního zásahu, včetně konfigurace biosu a samotného managementu. Vzdálený mount úložiště není dostatečný, z důvodu případné nízké propustnosti správcova připojení.

	· OOB karta serveru musí být schopna utvořit management skupinu s dalšími servery, tak aby prostředí mohlo být dohlíženo z jedné IP adresy bez nutnosti instalace externí management aplikace. Databáze takové skupiny musí být minimálně na dvou místech tak aby v případě výpadku jedné OOB karty, převzala funkcionalitu druhá v jiném serveru. Funkcionalita musí být alespoň v režimu master-slave (či active-pasive) a podporovat min. 100 serverů ve skupině	· OOB karta serveru je schopna utvořit management skupinu s dalšími servery, tak aby prostředí mohlo být dohlíženo z jedné IP adresy bez nutnosti instalace externí management aplikace. Databáze takové skupiny jsou minimálně na dvou místech tak aby v případě výpadku jedné OOB karty, převzala funkcionalitu druhá v jiném serveru. Funkcionalita musí být alespoň v režimu master-slave (či active-pasive) a podporovat min. 100 serverů ve skupině
	· OOB karta musí mít vestavěnu funkcionalitu automatického odeslání hrozících či vzniklých chybových stavů na helpdesk výrobce serverů a automatického vytvoření servisního incidentu, na základě, kterého se automaticky rozběhne servisní zásah (call-home)	· OOB karta má vestavěnu funkcionalitu automatického odeslání hrozících či vzniklých chybových stavů na helpdesk výrobce serverů a automatického vytvoření servisního incidentu, na základě, kterého se automaticky rozběhne servisní zásah (call-home)
	· možnost přístupu přes dedikovaný USB port s emulací síťového připojení	· možnost přístupu přes dedikovaný USB port s emulací síťového připojení
	· vzdálený reset, reboot s korektním ukončením OS, vypnutí a zapnutí serveru, včetně odpojení zdrojů (power cycle)	· vzdálený reset, reboot s korektním ukončením OS, vypnutí a zapnutí serveru, včetně odpojení zdrojů (power cycle)
	· management musí umožnit bezpečné smazání dat ze serveru a jeho médií pro případ vyřazení nebo přesunu serveru	· management umí umožnit bezpečné smazání dat ze serveru a jeho médií pro případ vyřazení nebo přesunu serveru

	· licence OOB managementu musí být pro server trvalá (life time), pokud je vyžadována. Výrobce udržuje databázi zakoupených licencí přístupnou kupujícímu, tak aby ji bylo možné v případě výměny HW kdykoliv obnovit, pokud dojte ke ztrátě	· licence OOB managementu je pro server trvalá (life time), pokud je vyžadována. Výrobce udržuje databázi zakoupených licencí přístupnou kupujícímu, tak aby ji bylo možné v případě výměny HW kdykoliv obnovit, pokud dojte ke ztrátě
	· management umožňuje monitoring spotřeby el. energie na úrovni serveru	· management umožňuje monitoring spotřeby el. energie na úrovni serveru
	· identifikace připojeného vzdáleného uživatele	· identifikace připojeného vzdáleného uživatele
	· vzdálená identifikace serveru	· vzdálená identifikace serveru
Bezpečnostní funkce	· Server musí být doručen s jedinečným HASH klíčem, který ověří neměnnost HW a SW komponent po celou dobu dopravního procesu z továrny výrobce až ke koncovému uživateli	· Server je doručen s jedinečným HASH klíčem, který ověří neměnnost HW a SW komponent po celou dobu dopravního procesu z továrny výrobce až ke koncovému uživateli

Podpora a servis	· Technická podpora a servis na 5 let (24x7x365), jediné kontaktní místo pro hlášení poruch pro všechny HW i SW komponenty dodávaného systému od výrobce. Technická podpora a servis je poskytován výrobcem HW. Zahájení servisních prací následující pracovní den od identifikace problému. Servis probíhá v místě instalace HW. Zdarma možnost stažení ovladačů a Firmware ze stránek výrobce pro konkrétní HW, po zadání jedinečného identifikátoru. Tato možnost stažení ovladačů a Firmware není omezena na dobu trvání technické podpory.	· Technická podpora a servis na 5 let (24x7x365), jediné kontaktní místo pro hlášení poruch pro všechny HW i SW komponenty dodávaného systému od výrobce. Technická podpora a servis je poskytován výrobcem HW. Zahájení servisních prací následující pracovní den od identifikace problému. Servis probíhá v místě instalace HW. Zdarma možnost stažení ovladačů a Firmware ze stránek výrobce pro konkrétní HW, po zadání jedinečného identifikátoru. Tato možnost stažení ovladačů a Firmware není omezena na dobu trvání technické podpory.
	· Zdarma přístup k aktualizacím firmware a ovladačů i po uplynutí doby platné podpory.	· Zdarma přístup k aktualizacím firmware a ovladačů i po uplynutí doby platné podpory.
	Prodávající se zavazuje, že zařízení a veškeré jeho komponenty:	Prodávající se zavazuje, že zařízení a veškeré jeho komponenty:
	· pochází z autorizovaného obchodního kanálu výrobce	· pochází z autorizovaného obchodního kanálu výrobce
	· je licencováno ve jménu kupujícího, včetně příslušného softwarového vybavení	· je licencováno ve jménu kupujícího, včetně příslušného softwarového vybavení
	· je reportováno zpět výrobci a kupující je uveden v databázi výrobce jako konečný uživatel	· je reportováno zpět výrobci a kupující je uveden v databázi výrobce jako konečný uživatel

SERVER BACKUP - časové zámky

Nabízený výrobek plní všechny požadované parametry.

SERVER BACKUP - časové zámky		
Název a výrobce	**Výrobce DELL** **Název: SERVER DELL PowerEdge R760 – konfigurace plnící všechny min. tech specifikace**	
Požadovaný počet : 1		
Technický parametr	Minimální technické požadavky	Popis splnění požadavku
Form Factor a vnitřní uspořádání	2U, pro přístup ke všem komponentám serveru není nutné nářadí, barevně značené hot-plug vnitřní komponenty a místa pro uchopení. Uzamykatelný přední panel.	2U, pro přístup ke všem komponentám serveru není nutné nářadí, barevně značené hot-plug vnitřní komponenty a místa pro uchopení. Uzamykatelný přední panel.
CPU	Dvousocketový systém založený na Intel platformě s využitím páté generace CPU Xeon. /AMD	Dvousocketový systém založený na Intel platformě s využitím páté generace CPU Xeon. /AMD
	Osazený 2x CPU s 8mi jádry, o základní frekvenci min. 2.6 GHz. Celkový výkon musí dosahovat minimálně 41400 bodů dle https://www.cpubenchmark.net	Osazený 2x CPU s 8mi jádry, o základní frekvenci min. 2.6 GHz. Celkový výkon dosahuje minimálně 41400 bodů dle https://www.cpubenchmark.net
RAM	8x 32GB na 5600MHz s možností osazení až 32 slotů.	8x 32GB na 5600MHz s možností osazení až 32 slotů.
Diskový subsystém	Server musí podporovat osazení min. 12x 3,5 palcových disků typu SAS/SATA, požadujeme server osazený hot-plug disky:	Server podporuje osazení min. 12x 3,5 palcových disků typu SAS/SATA, server osazený hot-plug disky:
	4x 12TB 7.2K RPM SATA 6Gbps 512e 3.5in Hot-plug Hard Drive	4x 12TB 7.2K RPM SATA 6Gbps 512e 3.5in Hot-plug Hard Drive
	Vlastní bootovací karta pro instalaci hypervizoru osazená minimálně:	Vlastní bootovací karta pro instalaci hypervizoru osazená minimálně:
	· 2x 480GB M.2 SSD NVMe v RAID1	· 2x 480GB M.2 SSD NVMe v RAID1

Diskový řadič	· typu SAS, PCI Express 4 kompatibilní, dvoukanálový (2 konektory)	· typu SAS, PCI Express 4 kompatibilní, dvoukanálový (2 konektory)
	· typu SAS, PCI Express 4 kompatibilní, dvoukanálový (2 konektory)	· typu SAS, PCI Express 4 kompatibilní, dvoukanálový (2 konektory)
	· podpora RAID 0, 1, 5, 6, 10, 50, 60	· podpora RAID 0, 1, 5, 6, 10, 50, 60
	· podpora 12Gbps technologie rozhraní disků	· podpora 12Gbps technologie rozhraní disků
	· podpora Capacity Expansion (OCE)	· podpora Capacity Expansion (OCE)
	· podpora RAID Level Migration (RLM)	· podpora RAID Level Migration (RLM)
	· podpora SED disků a SSD disků	· podpora SED disků a SSD disků
Síťové rozhraní	1 x 1GbE port Base-T (RJ45)	1 x 1GbE port Base-T (RJ45)
	1 x 10/25 GbE port Ethernet typu SFP28	1 x 10/25 GbE port Ethernet typu SFP28
	1 x 10 GbE port typu Base-T (RJ45)	1 x 10 GbE port typu Base-T (RJ45)
Napájení	Plně redundantní síťové napájecí zdroje 1100W s možností nastavení limitů výkonu a spotřeby v BIOSu (Power Budgeting) 96% účinnost při zatížení 50% (Titanium)	Plně redundantní síťové napájecí zdroje 1100W s možností nastavení limitů výkonu a spotřeby v BIOSu (Power Budgeting) 96% účinnost při zatížení 50% (Titanium)
Interface	· 3 x USB (1 vpředu, 2 vzadu), min. 1x USB 3.0	· 3 x USB (1 vpředu, 2 vzadu), min. 1x USB 3.0
	· 2 x VGA (1 vpředu, 1 vzadu)	· 2 x VGA (1 vpředu, 1 vzadu)
Rozšiřující sloty	· Min 3x PCIe Gen4/5 sloty volné pro budoucí použití	· Min 3x PCIe Gen4/5 sloty volné pro budoucí použití
Kolejnice	· Zásuvné ližiny s ramenem pro vedení kabelů	· Zásuvné ližiny s ramenem pro vedení kabelů
Kompatibilita	· Microsoft® Windows Server® 2019/2022, x64	· Microsoft® Windows Server® 2019/2022, x64
	· SUSE® Linux® Enterprise Server	· SUSE® Linux® Enterprise Server

	· Red Hat® Enterprise Linux	· Red Hat® Enterprise Linux
	· Canonical Ubuntu Server LTS	· Canonical Ubuntu Server LTS
	· VMware vSphere™	· VMware vSphere™
Operační systém	· Windows Datacenter 2022 – licence na všechna jádra	· Windows Datacenter 2022 – licence na všechna jádra
Management a vzdálená správa	· samostatný dedikovaný LAN RJ45 port, který se nezapočítává do konektivity serveru	· samostatný dedikovaný LAN RJ45 port, který se nezapočítává do konektivity serveru
	· s podporou failoveru na jinou síťovou kartu v serveru, musí podporovat VLAN a LLDP Discovery síťové infrastruktury, protokolů IPv4 a IPv6	· s podporou failoveru na jinou síťovou kartu v serveru, musí podporovat VLAN a LLDP Discovery síťové infrastruktury, protokolů IPv4 a IPv6
	· monitoring jakékoliv komponenty serveru nesmí vyžadovat instalaci agenta do OS, OS se musí kompletně obejít bez AMS (Agentless Management Service). Tento požadavek se týká i diskového systému, včetně přístupu k nastavení RAID řadičů, SAS HBA či případných expansních diskových polic serveru. V případě síťových karet na desce či mezzanine kartě, musí být v managementu možnost monitorování až do úrovně případných optický modulů (SFP) osazených v těchto kartách	· monitoring jakékoliv komponenty serveru nevyžaduje instalaci agenta do OS, OS se obejde bez AMS (Agentless Management Service). Tento požadavek se týká i diskového systému, včetně přístupu k nastavení RAID řadičů, SAS HBA či případných expansních diskových polic serveru. V případě síťových karet na desce či mezzanine kartě, musí být v managementu možnost monitorování až do úrovně případných optický modulů (SFP) osazených v těchto kartách
	· vestavěný HTML5 server pro správu bez nutnosti instalace ActiveX nebo Java pluginů, platí i pro vzdálenou konzoli KVM over IP	· vestavěný HTML5 server pro správu bez nutnosti instalace ActiveX nebo Java pluginů, platí i pro vzdálenou konzoli KVM over IP

	· management musí průběžně vyhodnocovat průměrné vytížení serveru s grafickým zobrazením v HTML5 GUI a možností alertů v případě excesů	· management průběžně vyhodnocuje průměrné vytížení serveru s grafickým zobrazením v HTML5 GUI a možností alertů v případě excesů
	· automatická instalace a obnova SSL certifikátu vestavěného serveru	· automatická instalace a obnova SSL certifikátu vestavěného serveru
	· přístup po SSL, Telnetu, SNMP a RESTful API s podporou Redfish SSE	· přístup po SSL, Telnetu, SNMP a RESTful API s podporou Redfish SSE
	· podpora multifaktorové autentizace, podpora MS AD a generického LDAP	· podpora multifaktorové autentizace, podpora MS AD a generického LDAP
	· možnost streamingu údajů senzorů serveru, telemetrie a reportů o provozu pro účely prediktivního vyhodnocování provozu a zabezpečení s podporou pro Splunk nebo ELK stack	· možnost streamingu údajů senzorů serveru, telemetrie a reportů o provozu pro účely prediktivního vyhodnocování provozu a zabezpečení s podporou pro Splunk nebo ELK stack
	· data logů musí být možné přesměrovat na sériový port RS232. Podpora Syslog serveru. Logy zaznamenávají stavy hardwarových sensorů (stav, teplota, napětí, …) včetně událostí o přihlášení a změnách konfigurace	· data logů je možné přesměrovat na sériový port RS232. Podpora Syslog serveru. Logy zaznamenávají stavy hardwarových sensorů (stav, teplota, napětí, …) včetně událostí o přihlášení a změnách konfigurace
	· podpora uzamčení stavu serveru pro zvýšení bezpečnosti (System Lock Down), automatický Secure OS recovery včetně BIOS serveru a firmware BMC, firmware rollback	· podpora uzamčení stavu serveru pro zvýšení bezpečnosti (System Lock Down), automatický Secure OS recovery včetně BIOS serveru a firmware BMC, firmware rollback

	· podpora dynamických změn nastavení externích USB portů systému, pro vzdálené povolení či zakázání portů, bez nutnosti restartu serveru či managementu	· podpora dynamických změn nastavení externích USB portů systému, pro vzdálené povolení či zakázání portů, bez nutnosti restartu serveru či managementu
	· podpora serverových konfiguračních profilů pro kompletně automatický deployment serverů vzdáleně i lokálně (Zero Touch deployment)	· podpora serverových konfiguračních profilů pro kompletně automatický deployment serverů vzdáleně i lokálně (Zero Touch deployment)
	· management musí umět poskytovat ovladače instalovaným operačním systémům bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS) a hardware firmware update s možností ověření a stažení aktuálních verzí proti online repository výrobce, případně zabezpečenému lokálnímu repository pod správou administrátora	· management umí poskytovat ovladače instalovaným operačním systémům bez speciální dedikované partition na interních discích serveru a nezávisle na těchto discích (úložiště nezávislé na OS) a hardware firmware update s možností ověření a stažení aktuálních verzí proti online repository výrobce, případně zabezpečenému lokálnímu repository pod správou administrátora
	· management musí umět poskytovat FW zařízením a kartám instalovaných v serveru, s možností automatické obnovy používané verze a konfigurace v případě výměny zařízení / karty z důvodu servisního zásahu, včetně konfigurace biosu a samotného managementu. Vzdálený mount úložiště není dostatečný, z důvodu případné nízké propustnosti správcova připojení.	· management umí poskytovat FW zařízením a kartám instalovaných v serveru, s možností automatické obnovy používané verze a konfigurace v případě výměny zařízení / karty z důvodu servisního zásahu, včetně konfigurace biosu a samotného managementu. Vzdálený mount úložiště není dostatečný, z důvodu případné nízké propustnosti správcova připojení.

	· OOB karta serveru musí být schopna utvořit management skupinu s dalšími servery, tak aby prostředí mohlo být dohlíženo z jedné IP adresy bez nutnosti instalace externí management aplikace. Databáze takové skupiny musí být minimálně na dvou místech tak aby v případě výpadku jedné OOB karty, převzala funkcionalitu druhá v jiném serveru. Funkcionalita musí být alespoň v režimu master-slave (či active-pasive) a podporovat min. 100 serverů ve skupině	· OOB karta serveru je schopna utvořit management skupinu s dalšími servery, tak aby prostředí mohlo být dohlíženo z jedné IP adresy bez nutnosti instalace externí management aplikace. Databáze takové skupiny jsou minimálně na dvou místech tak aby v případě výpadku jedné OOB karty, převzala funkcionalitu druhá v jiném serveru. Funkcionalita musí být alespoň v režimu master-slave (či active-pasive) a podporovat min. 100 serverů ve skupině
	· OOB karta musí mít vestavěnu funkcionalitu automatického odeslání hrozících či vzniklých chybových stavů na helpdesk výrobce serverů a automatického vytvoření servisního incidentu, na základě, kterého se automaticky rozběhne servisní zásah (call-home)	· OOB karta má vestavěnu funkcionalitu automatického odeslání hrozících či vzniklých chybových stavů na helpdesk výrobce serverů a automatického vytvoření servisního incidentu, na základě, kterého se automaticky rozběhne servisní zásah (call-home)
	· možnost přístupu přes dedikovaný USB port s emulací síťového připojení	· možnost přístupu přes dedikovaný USB port s emulací síťového připojení
	· vzdálený reset, reboot s korektním ukončením OS, vypnutí a zapnutí serveru, včetně odpojení zdrojů (power cycle)	· vzdálený reset, reboot s korektním ukončením OS, vypnutí a zapnutí serveru, včetně odpojení zdrojů (power cycle)
	· management musí umožnit bezpečné smazání dat ze serveru a jeho médií pro případ vyřazení nebo přesunu serveru	· management umí umožnit bezpečné smazání dat ze serveru a jeho médií pro případ vyřazení nebo přesunu serveru

	· licence OOB managementu musí být pro server trvalá (life time), pokud je vyžadována. Výrobce udržuje databázi zakoupených licencí přístupnou kupujícímu, tak aby ji bylo možné v případě výměny HW kdykoliv obnovit, pokud dojte ke ztrátě	· licence OOB managementu je pro server trvalá (life time), pokud je vyžadována. Výrobce udržuje databázi zakoupených licencí přístupnou kupujícímu, tak aby ji bylo možné v případě výměny HW kdykoliv obnovit, pokud dojte ke ztrátě
	· management umožňuje monitoring spotřeby el. energie na úrovni serveru	· management umožňuje monitoring spotřeby el. energie na úrovni serveru
	· identifikace připojeného vzdáleného uživatele	· identifikace připojeného vzdáleného uživatele
	· vzdálená identifikace serveru	· vzdálená identifikace serveru
Bezpečnostní funkce	· Server musí být doručen s jedinečným HASH klíčem, který ověří neměnnost HW a SW komponent po celou dobu dopravního procesu z továrny výrobce až ke koncovému uživateli	· Server je doručen s jedinečným HASH klíčem, který ověří neměnnost HW a SW komponent po celou dobu dopravního procesu z továrny výrobce až ke koncovému uživateli

Podpora a servis	· Technická podpora a servis na 5 let (24x7x365), jediné kontaktní místo pro hlášení poruch pro všechny HW i SW komponenty dodávaného systému od výrobce. Technická podpora a servis je poskytován výrobcem HW. Zahájení servisních prací následující pracovní den od identifikace problému. Servis probíhá v místě instalace HW. Zdarma možnost stažení ovladačů a Firmware ze stránek výrobce pro konkrétní HW, po zadání jedinečného identifikátoru. Tato možnost stažení ovladačů a Firmware není omezena na dobu trvání technické podpory.	· Technická podpora a servis na 5 let (24x7x365), jediné kontaktní místo pro hlášení poruch pro všechny HW i SW komponenty dodávaného systému od výrobce. Technická podpora a servis je poskytován výrobcem HW. Zahájení servisních prací následující pracovní den od identifikace problému. Servis probíhá v místě instalace HW. Zdarma možnost stažení ovladačů a Firmware ze stránek výrobce pro konkrétní HW, po zadání jedinečného identifikátoru. Tato možnost stažení ovladačů a Firmware není omezena na dobu trvání technické podpory.
	· Zdarma přístup k aktualizacím firmware a ovladačů i po uplynutí doby platné podpory.	· Zdarma přístup k aktualizacím firmware a ovladačů i po uplynutí doby platné podpory.
	Prodávající se zavazuje, že zařízení a veškeré jeho komponenty:	Prodávající se zavazuje, že zařízení a veškeré jeho komponenty:
	· pochází z autorizovaného obchodního kanálu výrobce	· pochází z autorizovaného obchodního kanálu výrobce
	· je licencováno ve jménu kupujícího, včetně příslušného softwarového vybavení	· je licencováno ve jménu kupujícího, včetně příslušného softwarového vybavení
	· je reportováno zpět výrobci a kupující je uveden v databázi výrobce jako konečný uživatel	· je reportováno zpět výrobci a kupující je uveden v databázi výrobce jako konečný uživatel

Diskové Pole

Nabízený výrobek plní všechny požadované parametry.

Pole		
Název a výrobce	**Výrobce DELL** **Název: Dell ME5024 Storage – konfigurace plnící všechny min. tech specifikace**	
Požadovaný počet : 1		
Technický parametr	Minimální technické požadavky	Popis splnění požadavku
Typ zařízení	· Diskové pole, v provedení do rack 19“ o maximální velikosti 2U. S blokovým přístupem.	· Diskové pole, v provedení do rack 19“ o maximální velikosti 2U. S blokovým přístupem.
	· Multikontrolerové řešení s plně redundantní, vysoce dostupnou architekturou bez SPOF (Single Point of Failure), umožňující upgrade FW za provozu, řadiče v režimu Active-Active. S podporou SAS SSD a HDD disků a NL-SAS disků.	· Multikontrolerové řešení s plně redundantní, vysoce dostupnou architekturou bez SPOF (Single Point of Failure), umožňující upgrade FW za provozu, řadiče v režimu Active-Active. S podporou SAS SSD a HDD disků a NL-SAS disků.
Diskový subsystém	· Minimálně osazeno disky 12x 1.92TB 2.5“ SAS SSD min. Disky min DWPD 1.	· Minimálně osazeno disky 12x 1.92TB 2.5“ SAS SSD min. Disky min DWPD 1.
	· Diskové pole musí podporovat výměnu všech HDD za běhu (tzv. hot swap) a podporovat global spare HDD, případně spare prostor	· Diskové pole podporuje výměnu všech HDD za běhu (tzv. hot swap) a podporovat global spare HDD, případně spare prostor
	· Celková rozšiřitelnost datového úložiště minimálně na 270 disků, připojením pouze expanzních jednotek pro disky.	· Celková rozšiřitelnost datového úložiště minimálně na 270 disků, připojením pouze expanzních jednotek pro disky.
	· Možnost připojovat expanzní jednotky na disky o velikostech 2,5“ a 3,5“	· Možnost připojovat expanzní jednotky na disky o velikostech 2,5“ a 3,5“

RAID	· Diskové pole musí mít podporu pro RAID 1, 5, 6, 10 a distribuovaný erasure coding odpovídající RAID6	· Diskové pole musí mít podporu pro RAID 1, 5, 6, 10 a distribuovaný erasure coding odpovídající RAID6
Počet řadičů	· Min. 2 řadiče/kontroléry diskového pole	· Min. 2 řadiče/kontroléry diskového pole
Cache	· Velikost operační paměti (cache) typu RAM - minimálně 32 GB a současně minimálně 16 GB na řadič pro data.	· Velikost operační paměti (cache) typu RAM - minimálně 32 GB a současně minimálně 16 GB na řadič pro data.
Back-end	· Typ připojení Back-endu pro expanzní police min. SAS 3.0 12 Gb/s, vyžadovány jsou minimálně dva SAS 3.0, 12 Gb/s porty na každý controller.	· Typ připojení Back-endu pro expanzní police min. SAS 3.0 12 Gb/s, vyžadovány jsou minimálně dva SAS 3.0, 12 Gb/s porty na každý controller.
Front-end porty	· Počet a typ front-end portů – požadujeme minimálně 4x 32FC per controller. Vyžadujeme podporu přímého zapojení nabízeného pole s nabízenými servery. Součástí nabídky musí být i kompatibilní propojovací transceivery a kabely o minimální délce 2 m min. 2ks na každý server.	· Počet a typ front-end portů – minimálně 4x 32FC per controller. podpora přímého zapojení nabízeného pole s nabízenými servery. Součástí nabídky jsou i kompatibilní propojovací transceivery a kabely o minimální délce 2 m min. 2ks na každý server.
Napájení	2 redundantní zdroje PDU koncovky	2 redundantní zdroje PDU koncovky
LUN	· Celkový počet LUNů na diskovém poli - min. 500.	· Celkový počet LUNů na diskovém poli - min. 500.
	· Podpora LUNů o min. velikosti 50 TiB	· Podpora LUNů o min. velikosti 50 TiB
	· Min. 1ks GE Management port, na řadič	· Min. 1ks GE Management port, na řadič

Požadované vlastnosti managementu diskového pole	· Grafické uživatelské rozhraní včetně licence pro lokální správu diskového pole a příkazové řádky (CLI), mapování jednotlivých interních rolí a oprávnění na uživatelské skupiny v adresářové službě LDAP, výkonnostní statistiky, které lze exportovat v čitelném formátu (CSV/XML apod.) pomocí CLI nebo GUI	· Grafické uživatelské rozhraní včetně licence pro lokální správu diskového pole a příkazové řádky (CLI), mapování jednotlivých interních rolí a oprávnění na uživatelské skupiny v adresářové službě LDAP, výkonnostní statistiky, které lze exportovat v čitelném formátu (CSV/XML apod.) pomocí CLI nebo GUI
	· Možnost zasílat události s různými severitami, které vznikají spontánně uvnitř pole za běžného provozu (např. chybové stavy, přihlášení uživatele apod.), pomocí standardních protokolů SMTP nebo SNMP	· Možnost zasílat události s různými severitami, které vznikají spontánně uvnitř pole za běžného provozu (např. chybové stavy, přihlášení uživatele apod.), pomocí standardních protokolů SMTP nebo SNMP
	· Automatické hlášení poruch a problémů pomocí e-mailu, nebo automaticky na dohled dodavatele přes internet zabezpečeně	· Automatické hlášení poruch a problémů pomocí e-mailu, nebo automaticky na dohled dodavatele přes internet zabezpečeně
	· Jednotná grafická konzole pro správu a monitoring serverů i diskového pole, s možností napojení do proaktivního monitoringu s prediktivní analýzou, v cloudového portálu výrobce. Tento portál přístupný i přes mobilní aplikace dostupné pro telefony iOS i Android. Pokud jsou vyžadovány licence musí být součástí řešení, minimálně po dobu platné podpory.	· Jednotná grafická konzole pro správu a monitoring serverů i diskového pole, s možností napojení do proaktivního monitoringu s prediktivní analýzou, v cloudového portálu výrobce. Tento portál přístupný i přes mobilní aplikace dostupné pro telefony iOS i Android. Pokud jsou vyžadovány licence musí být součástí řešení, minimálně po dobu platné podpory.

Funkce a licence	· Součástí musí být SW licencovaný v rozsahu pro maximální kapacitu pole, a to včetně rozšiřitelnosti kapacity):	· Součástí je SW licencovaný v rozsahu pro maximální kapacitu pole, a to včetně rozšiřitelnosti kapacity):
	· kompletní správa diskového pole,	· kompletní správa diskového pole,
	· licence pro plně automatický sub-LUN tiering dat s 3 tier architekturou,	· licence pro plně automatický sub-LUN tiering dat s 3 tier architekturou,
	· licence pro snapshoty, klony, asynchronní replikaci, šifrování při použití SED disků a SSD cache musí být součástí	· licence pro snapshoty, klony, asynchronní replikaci, šifrování při použití SED disků a SSD cache je součástí
	· dlouhodobý performance monitoring a reporting, a to až po dobu 6 měsíců,	· dlouhodobý performance monitoring a reporting, a to až po dobu 6 měsíců,
	· Thin Provisioning,	· Thin Provisioning,
	· zástupnost datových cest (multi-path) pokud pole nepoužívá standardní MPIO ovladače,	· zástupnost datových cest (multi-path) pokud pole nepoužívá standardní MPIO ovladače,
	· kopírování jednotlivých LUNů v rámci pole i mezi jednotlivými diskovými poli,	· kopírování jednotlivých LUNů v rámci pole i mezi jednotlivými diskovými poli,
	· minimálně 1024 Snapshotů.	· minimálně 1024 Snapshotů.

Záruka	Podpora na 5 let typu 24x7x365 s dobou zahájení opravy do 4h od nahlášení poruchy, oprava v místě instalace serveru, servis je poskytován výrobcem. Jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému. Možnost stažení ovladačů a management software na webových stránkách výrobce po zadání unikátního sériového čísla.	Podpora na 5 let typu 24x7x365 s dobou zahájení opravy do 4h od nahlášení poruchy, oprava v místě instalace serveru, servis je poskytován výrobcem. Jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému. Možnost stažení ovladačů a management software na webových stránkách výrobce po zadání unikátního sériového čísla.

NAS

NAS (backup Office 365)		
Název a výrobce	**Výrobce: Synology** **Název: NAS RS1221+ Rack Station (plnící všechna min parametry) + 4x Synology HAT5300/16TB/HDD/3.5"/SATA/7200 RPM/5R**	
Technický parametr	Minimální technické požadavky	Popis splnění požadavku
montaz	RACK	RACK
CPU	AMD Ryzen V1500B	AMD Ryzen V1500B
Systémová paměť:	32 GB DDR4 ECC SODIMM	32 GB DDR4 ECC SODIMM
Šachty pevného disku:	8	8
Maximální počet šachet pevného disku s rozšiřující jednotkou:	12	12
Hot-swap disk:	ano	ano
Porty:	4x RJ-45 1GbE LAN Port s podporou funkcí Link Aggregation / Failover 2x USB 3.2 Gen 1 1x eSATA 1x 10GbE 2x PCIe NVMe	4x RJ-45 1GbE LAN Port s podporou funkcí Link Aggregation / Failover 2x USB 3.2 Gen 1 1x eSATA 1x 10GbE 2x PCIe NVMe
HDD	4x 16TB, 3.5", SATA, 7200 RPM - podpora vyrobce NAS	4x 16TB, 3.5", SATA, 7200 RPM - podpora vyrobce NAS
Požadavky na podporu výrobcem	**ANO/NE**	**Popis splnění požadavku**
Podpora výrobce na 5 let		Podpora výrobce na 5 let

UPS - páteřní prvky

Nabízený výrobek plní všechny požadované parametry.

UPS - páteřní prvky		
Požadovaný počet : 2		
Název a výrobce	**Výrobce: APC** **Název: APC Smart-UPS 3000VA LCD RM 2U 230V with SmartConnect**	
Technický parametr	Minimální technické požadavky	Popis splnění požadavku
montáž	RACK	RACK
Kapacita výstupního výkonu [VA]:	3000	3000
Topologie:	Line interaktivní	Line interaktivní
Typ křivky:	Sinusoida	Sinusoida
Jmenovité vstupní napětí [V]:	230 V	230 V
Typ připojení vstupu:	British BS1363A, IEC-320 C20, Schuko CEE 7/EU1-16P	British BS1363A, IEC-320 C20, Schuko CEE 7/EU1-16P
KOMUNIKACE A SPRÁVA		
Port rozhraní:	RJ-45 10/100 Base-T, RJ-45 Serial, SmartSlot, USB	RJ-45 10/100 Base-T, RJ-45 Serial, SmartSlot, USB
Ovládací panel:	diody zobrazují stav: napájení ze sítě : napájení z baterie : vyměnit baterii : přetížen	diody zobrazují stav: napájení ze sítě : napájení z baterie : vyměnit baterii : přetížen
Zvukové upozornění:	Upozornění na stav, kdy je systém napájen z baterie	Upozornění na stav, kdy je systém napájen z baterie
Požadavky na podporu	**ANO/NE**	**Popis splnění požadavku**
Podpora výrobce na 5 let	ANO	Podpora výrobce na 5 let

Zálohovací software

Zálohovací software		
Název a výrobce	**Výrobce: VEEAM** **Název: Veeam Data Platform Essentials Universal Subscription License. Includes Enterprise Plus Edition features.**	
Technický parametr	Minimální technické požadavky	Popis splnění požadavku
popis	**Min. na úrovni funkcí sw. Veeam**	
Zálohování na úrovni hypervisoru per VM	ANO	Zálohování na úrovni hypervisoru per VM
Agentové zálohování	ANO	Agentové zálohování
Počet virtuálních strojů	**20**	Počet virtuálních strojů 20
Požadavky na podporu	**ANO/NE**	**Popis splnění požadavku**
Servisní a uživatelská podpora v délce 5 let	ANO	**Servisní a uživatelská podpora v délce 5 let**

licence

licence		
Technický parametr	Minimální počet	Popis splnění požadavku
CSP Windows Server 2022 - 1 Device CAL EDU	200	200
CSP Windows Server 2022 Remote Desktop Services - 1 User CAL EDU	15	15
CSP Windows Server 2022 Datacenter - 16 Core EDU	licence na všechna jádra nabízených serveru	licence na všechna jádra nabízených serveru (4x16core)

implementace

Instalace serverové infrastruktury a zálohování		
Technický parametr	**Specifikace – minimální požadavek zadavatele**	Naplnění požadavku
Instalace	Instalace hypervisoru na servery	Instalace hypervisoru na servery
Instalace	Konfigurace síťového připojení	Konfigurace síťového připojení
Instalace	Instalace a konfigurace diskového pole,	Instalace a konfigurace diskového pole,
Instalace	Nastavení virtuálních strojů, předpokládáme 2xVM na produkčních serverech + virtualizace na backup server	Nastavení virtuálních strojů, předpokládáme 2xVM na produkčních serverech + virtualizace na backup server
Instalace	Instalace HDD do NAS, nastavení	Instalace HDD do NAS, nastavení
Instalace	Zálohovací plány - návrh a konfigurace	Zálohovací plány - návrh a konfigurace
Instalace	Konfigurace switchů	Konfigurace switchů
Instalace	Rozděleni VLAN	Rozděleni VLAN
Instalace	migrace a nastavení	migrace a nastavení
Instalace	akceptační testy a testovací provoz	akceptační testy a testovací provoz
školení	školení administrátorů v rozsahu 4 hodin	školení administrátorů v rozsahu 4 hodin
dokumentace	dokumentace skutečného provedení	dokumentace skutečného provedení

ID003 - Ochrana koncových stanic ENDPOINT

v současnosti zalicencováno 120 zařízení stanice/servery licence ESET PROTECT Entry on-prem.
Zadavatel požaduje konkrétní produkt z důvodu zachování kompatibility, resp. navazujícího přechodu na vyšší verzi s funkcionalitou EDR.

ID licence: 33D-FPK-78C.

Ochrana koncových stanic a SVR		
Název a výrobce	**Výrobce. ESET** **Název: PROTECT ELITE**	
Požadovaný počet : 120		
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
Správcovská konzole - Kybernetická platforma poskytující přehled o dění v síti a kontrolu nad ní. Může být nainstalována jako cloudové nebo lokální řešení.	ANO	Správcovská konzole - Kybernetická platforma poskytující přehled o dění v síti a kontrolu nad ní. Může být nainstalována jako cloudové nebo lokální řešení.
ochrana koncových zařízení	ANO	ochrana koncových zařízení
Antivirus poskytuje ochranu před známými i novými hrozbami. Přístup založený na umělé inteligenci a prevenci	ANO	Antivirus poskytuje ochranu před známými i novými hrozbami. Přístup založený na umělé inteligenci a prevenci
Ochrana proti síťovým útokům	ANO	Ochrana proti síťovým útokům
Správa zařízení - Umožňuje omezení přístupu neautorizovaných zařízení, jako jsou USB flash disky nebo CD, k citlivým datům	ANO	Správa zařízení - Umožňuje omezení přístupu neautorizovaných zařízení, jako jsou USB flash disky nebo CD, k citlivým datům
Anti-phishing	ANO	Anti-phishing
Ochrana serverů - Ochrana dat v reálném čase pro všechny běžné servery.	ANO	Ochrana serverů - Ochrana dat v reálném čase pro všechny běžné servery.
Ochrana mobilních zařízení proti hrozbám - mobilní zařízení s Androidem a iOS. Funkce antimalware, anti-theft a MDM.	ANO	Ochrana mobilních zařízení proti hrozbám - mobilní zařízení s Androidem a iOS. Funkce antimalware, anti-theft a MDM.
Šifrování celého disku	ANO	Šifrování celého disku

Pokročilá ochrana před hrozbami - Proaktivní cloudová ochrana proti ransomwaru a dosud neznámým hrozbám se schopností automatické nápravy.	ANO	Pokročilá ochrana před hrozbami - Proaktivní cloudová ochrana proti ransomwaru a dosud neznámým hrozbám se schopností automatické nápravy.
Rozšířená detekce a reakce - umožňuje aktivní detekci hrozeb, efektivní identifikaci neobvyklého chování v síti a včasnou nápravu. Nástroj podporující využití XDR v cloudu.	ANO	Rozšířená detekce a reakce - umožňuje aktivní detekci hrozeb, efektivní identifikaci neobvyklého chování v síti a včasnou nápravu. Nástroj podporující využití XDR v cloudu.
Požadavky na podporu výrobcem	**ANO/NE**	**Popis splnění požadavku**
Podpora výrobce na 5 let	ANO	Podpora výrobce na 5 let

implementace

Ochrana koncových stanic a SVR		
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
migrace a nastavení	ANO	migrace a nastavení
akceptační testy a testovací provoz	ANO	akceptační testy a testovací provoz
školení administrátorů v rozsahu 2 hodin	ANO	školení administrátorů v rozsahu 2 hodin
dokumentace skutečného provedení	ANO	dokumentace skutečného provedení

ID004 - Analýza sítového provozu (ochrana integrity sítě školy)

Analýza sítového provozu poskytne pro ochranu tohoto IS úplný a přesný přehled o dění ve vaší síti. V případě ohrožení provozu tohoto IS, lze tuto hrozbu detekovat. Použití této nejmodernější techniky detekce a dojde k bezprostřednímu řešení známých i neznámých hrozeb a problémů, kterým by mohla být síť vystavena. Analýza sítového provozu používá pokročilé techniky umělé inteligence a strojového učení, aby odhalil nebezpečí a slabá místa v infrastruktuře, která nelze detekovat klasickými bezpečnostními produkty. Zastaví útoky na školní síť, pomůže i obecně s moderními formami kybernetické kriminality i s nedostatky vedoucími k nestabilitě sítě. Jeho nasazení předchází finančním škodám na nedostupnosti IS, časovým ztrátám a zvýšeným nákladům na lidské zdroje či externí služby

Analýza sítového provozu		
Název a výrobce	**Výrobce: GREYCORTEX Typ: Mendel AIO**	
Minimální technické požadavky	Technický parametr	Popis splnění požadavku
Požadavky na monitorovací systém		
Ucelené škálovatelné řešení umožňující dlouhodobé monitorování sítě na bázi technologie datových toků (NetFlow, IPFIX, jFlow, cflowd, NetStream, cloudové FlowLogy).	Ucelený, škálovatelný NetFlow/IPFIX/FlowLogs monitorovací systém	ANO / Nabízené řešení je škálovatelné a umožňuje dlouhodobě monitorovat síť na základě datových toků
Podpora IPv4, IPv6, VLAN, MPLS, Ethernet 10Mb/s až 100Gb/s.	Podpora infrastruktury	ANO / Podporuje uvedené parametry infrastruktury.

Sběr síťových statistik ze vzdálených lokalit s centrálním přístupem k reportům, incidentům a síťovým statistikám a centrální správou systému.	Decentralizovaný monitoring lokalit s centrální správou	ANO / Nabízené řešení umožňuje decentralizovaný monitoring lokalit s centrální správou
Nezávislost na stávající síťové infrastruktuře (optické či metalické datové rozvody) a použitých aktivních prvcích (typ nebo výrobce).	Nezávislost na stávající infrastruktuře	ANO / Nabízené řešení je zcela nezávislé na stávající síťové infrastruktuře
Bezztrátový sběr dat na kolektorech z různých datových zdrojů, podpora standardizovaných protokolů pro výměnu dat o IP tocích (NetFlow v5, NetFlow v9 – RFC3954, IPFIX, jFlow, cflowd, NetStream).	Bezztrátový sběr flow statistik z více zdrojů	ANO / Řešení umožňuje bezztrátový sběr dat z různých datových zdrojů a podporuje uvedené standardizované protokoly.
Dlouhodobé ukládání statistik IP toků a jejich centrální sledování a vyhodnocování bezpečnostních hrozeb v síti, prokazování bezpečnostních incidentů.	Ukládání statistik a vyhodnocování bezpečnostních hrozeb	ANO / Řešení ukládá statistiky IP toků a centrálně sleduje a vyhodnocuje bezpečnostní hrozby v síti.
Plná zákaznická podpora v českém jazyce.	Zákaznická podpora	ANO / Řešení je podporováno v českém jazyce.
Systém ověřený instalacemi v rozsáhlé síťové infrastruktuře (datové linky 10 Gbps a výše). Minimálně 10 instalací ve třech zemích světa.	Reference	ANO / Řešení je léty ověřené u řady zákazníků v mnoha zemích Evropy, Asie a také v dalších částech světa. Je nasazeno i v infrastrukturách až s 100 Gbps linkami. Veřejné reference jsou k dohledání na veřejných zdrojích.
Otevřené rozhraní a veřejně dokumentované API s možností integrace nástrojů i třetích stran.	Rozhraní pro integraci nástrojů třetích stran	ANO / Řešení poskytuje otevřené rozhraní s možností integrace nástrojů třetích stran.
Monitorovací systém sleduje aktivní relace všech uživatelů a umožnuje tyto relace ukončit.	Správa aktivních relací uživatelů s monitorovacím systémem	ANO / Řešení sleduje aktivní relace všech uživatelů a umožňuje je ukončit.
Během aktualizace systém zabraňuje uživatelským akcím, které by mohly narušit proces aktualizace.	Uzamčení rozhraní během aktualizací	ANO / Řešení umožňuje zabránit uživatelským akcím, které by proces mohly narušit.

Požadavky na kolektory NetFlow dat		
Minimální technické požadavky	Technický parametr	Popis splnění požadavku
Zabezpečené kolektory flow statistik s databází pro plné uložení síťových statistik na multigigabitových linkách bez jakékoliv redukce.	Ukládání flow statistik	ANO / Řešení je navrženo tak, že kolektor ukládá síťové statistiky bez jakékoliv redukce.
Kolektor umožní zpracování a vizualizaci flow záznamů volitelně v 5 minutových, 1 minutových nebo 30 sekundových intervalech, přičemž tuto hodnotu lze samostatně nastavit per definovaný síťový rozsah nebo definovanou množinu toků.	Granularita vizualizace	ANO / Kolektor umožňuje zpracování a vizualizaci ve volitelných časových intervalech; hodnotu lze nastavit definováním síťového rozsahu nebo množiny toků.
Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream, sFlow, NetFlow Lite. Podpora VPC flow logů z AWS, Azure a GCP.	Podpora standardů datových toků	ANO / Nabízené řešení podporuje uvedené standardy síťových toků.
Možnost dohledání libovolné komunikace až na úroveň jednotlivých flow záznamů, průběžné grafy provozu, top statistiky, reporty, alerty, databáze aktivních zařízení na síti vč. identifikace zařízení.	Hlavní funkcionalita	ANO / Řešení umožňuje dohledání komunikace až na úroveň flow záznamů, grafů provozu, top statistik, reportů, alertů a databází aktivních zařízení v síti včetně identifikace zařízení.
Snadná instalace do stávající síťové infrastruktury – racková montáž nebo šablony pro nasazení virtuálního stroje.	Instalace	ANO / Řešení umožňuje snadnou instalaci do síťové infrastruktury - umístění do racku (v případě dedikovaného HW), případně na virtuální stroj (SW appliance).
Jednoduchá konfigurace pomocí dostupných konfiguračních šablon, které umožňují výběr z dostupných “Presets” a jejich aplikací vytvářet profily, kapitoly, reporty, alerty, widgety a dashboardy bez nutnosti manuální konfigurace.	Konfigurační šablony	ANO / Řešení umožňuje snadnou konfiguraci výběrem z předpřipravených konfiguračních šablon a jejich prostřednictvím vytvářet profily, kapitoly, reporty, alerty, widgety a dashboardy bez nutnosti manuální konfigurace.

Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS.	Zabezpečená vzdálená správa	ANO / Řešení umožňuje vzdálenou správu, dohled a konfiguraci SSH a HTTPS.
Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. Separace dat s omezením přístupu pro jednotlivé role/uživatele.	Správa uživatelů a přístupových práv	ANO / Řešení umožňuje správu uživatelů a přístupových práv prostřednictvím uživatelských rolí.
Podpora autentizace vůči LDAP (Active Directory).	LDAP autentizace	ANO / Řešení podporuje LDAP autentizaci.
Podpora autentizace vůči TACACS+.	TACACS+ autentizace	ANO / Řešení umožňuje podporu autentizace vůči TACACS+.
Kolektor je možné integrovat do dohledového systému pro kontrolu dostupnosti a vytížení zdrojů technologií SNMP.	Dohled	ANO / Kolektor lze integrovat do dohledu pro kontrolu dostupnosti a vytížení zdrojů SNMP.
Časová synchronizace zařízení proti centrálnímu zdroji času na síti.	Časová synchronizace	ANO / Řešení umožňuje časovou synchronizaci zařízení vůči centrálnímu zdroji času v síti.
Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky.	Podpora příkazové řádky	ANO / Řešení lze jednoduše instalovat, nastavit i spravovat přes příkazovou řádku.
Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména.	DNS cache	ANO / Řešení umožňuje použít DNS cache na zařízení pro překlad IP adres na doménová jména.
Podpora IPFIX položek proměnlivé délky.	Podpora položek proměnlivé délky	ANO / Řešení podporuje IPFIX položky proměnlivé délky.
Podpora rozšíření VMware NSX, Gigamon a Ixia IPFIX Extensions.	Podpora IPFIX rozšíření jiných výrobců	ANO / Řešení podporuje IPFIX rozšíření jiných výrobců.
Sběr a analýza RTT, SRT, delay, jitter, retransmise, out-of-order pakety.	Monitoring výkonu sítě	ANO / Řešení umožňuje monitoring uvedených parametrů výkonu sítě.
Podpora pro protokoly HTTP, VoIP SIP, DNS, SMB/CIFS, DHCP, SMTP, POP3, IMAP a MS SQL (TDS). Systém umožňuje extrahovat SNI (Server Name Indication) z HTTPS a QUIC protokolů.	Monitoring informací z aplikační vrstvy	ANO / Řešení podporuje uvedené protokoly pro monitoring informací z aplikační vrstvy.

Podpora pro monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících identifikaci NATů.	Monitorování rozšířených L3/L4 informací	ANO / Řešení podporuje monitorování uvedených rozšířených L3/L4 informací.
Časové známky je možné přidat do flow záznamů, které tuto informaci nemají od zdroje flow záznamů.	Automatická korekce časových známek	ANO / Řešení umožňuje přidat do flow záznamů časové známky.
Systém je schopen sbírat a ukládat dlouhodobě data z tisíců zdrojů flow dat. Disková kapacita datového úložiště musí umožnit záznamy statistik bez jakékoliv redukce v horizontu minimálně šesti měsíců.	Kapacita datového úložiště	ANO / Řešení je navrženo tak, aby umožnilo záznamy statistik bez redukce na 6 měsíců.
Systém podporuje rozdílné samplovací (vzorkovací) poměry pro každé rozhraní u jednotlivých zdrojů flow dat.	Rozlišování rozdílných samplovacích poměrů pro každé rozhraní zdroje flow dat	ANO / Řešení podporuje rozdílné vzorkovací poměry pro každé rozhraní zdroje flow.
Možnost přeposílání přijímaných flow statistik ke zpracování na další kolektory včetně možnosti samplování na úrovni datových toků. Možnost převodu formátu (NetFlow v5/v9, IPFIX) přeposílaných flow statistik.	Přeposílání flow vč. možnosti samplingu a převodu formátu	ANO / Řešení umožňuje přeposílání flow včetně možnosti vzorkování a převodu uvedených formátů.
Přijímání a přeposílání IPFIX dat pomocí spolehlivého TCP spojení s možností šifrování (TCP/TLS) dle standardu RFC 7011.	Spolehlivý a šifrovaný přenos IPFIX dat	ANO / Řešení umožňuje příjem a přeposílání IPFIX pomocí spolehlivého TCP spojení.
Kolektor automaticky identifikuje každý zdroj flow statistik, který mu tyto statistiky zasílá ke zpracování. O daném zdroji získá základní informace jako název, počet a rychlost rozhraní. Pro každý zdroj flow statistik automaticky zobrazuje graf průběhu provozu.	Automatická identifikace zdroje flow statistik	ANO / Kolektor automaticky identifikuje zdroje flow statistik, včetně uvedených informací.
Kolektor automaticky detekuje výpadky nebo výrazné poklesy v příjmu dat od jednotlivých zdrojů flow dat.	Identifikace výpadku dat	ANO / Kolektor automaticky detekuje výpadky/poklesy v příjmu dat.

Flow statistiky je možné automaticky zálohovat na externí síťové úložiště z důvodu dlouhodobé archivace. Zálohované statistiky lze v případě potřeby přímo obnovit uživatelem do kolektoru, kde je možné tyto statistiky analyzovat standardními prostředky.	Zálohování a obnova flow statistik	ANO / Řešení umožňuje automaticky zálohovat flow statistiky na externí úložiště pro archivaci; tyto lze obnovit uživatelem do kolektoru.
Kolektor umožňuje zobrazení přihlášeného uživatele u daného zařízení (IP adresy) včetně historie. Flow statistiky je možné filtrovat na základě loginu uživatele. Uživatelské identity jsou získávány ze systémů řízení přístupu do sítě (např. Cisco ISE) nebo Active Directory. Řešení je otevřené a schopné podporovat libovolný zdroj uživatelských identit (hlášení o úspěšné autentizaci uživatele).	Podpora pro uživatelské identity	ANO / Kolektor umožňuje zobrazit identitu uživatele včetně historie využitím se systému řízení přístupu do sítě.
Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard s podporou více záložek (konfigurace per uživatel).	Uživatelské rozhraní	ANO / Řešení poskytuje webové GUI v českém jazyce a uživatelsky definovatelný dashboard.
Systém obsahuje předdefinované dashboardy, které uživatel může použít při vytváření dashboardu. Uživatel může vytvořený dashboard označit jako předdefinovaný, čímž je přidán do seznamu předdefinovaných dashboardů.	Předdefinované dashboardy	ANO / Řešení obsahuje předdefinované dashboardy, které lze využít pro vlastní uživatelské dashboardy.
Uživatel může sdílet dashboard s dalšími uživateli nebo uživatelskými rolemi, kteří si mohou sdílený dashboard zobrazit (případně i editovat).	Sdílené dashboardy	ANO / Řešení umožňuje uživateli sdílet dashboard s dalšími uživateli / rolemi pro zobrazení i editaci.
Vytváření dlouhodobých grafů a přehledů s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH),	Vizualizace statistických dat	ANO / Řešení umožňuje vytváření grafů a přehledů s různými typy pohledů dle uvedených kategorií včetně uživatelské konfigurace.

včetně plné konfigurace grafů a pohledů uživatelem.		
Vizualizace výkonnostních metrik sítě v grafech provozu společně s volumetrickými statistikami.	Vizualizace výkonnostních metrik sítě	ANO / Řešení umožňuje vizualizaci výkonnostních metrik sítě v grafech provozu s volumetrickými statistikami.
Zařízení vizualizuje výkonnostní metriky sítě (např. doba zpoždění sítě RTT, doba zpoždění serveru SRT) vykreslováním křivek do průběhového grafu síťového provozu. Při označení časového intervalu jsou zobrazeny průměrné hodnoty výkonnostních metrik bez potřeby spuštění dotazu nad uloženými flow statistikami v kolektoru.	Vizualizace výkonnostních metrik sítě	ANO / Řešení umožňuje vizualizaci uvedenou vizualizaci výkonnostních metrik sítě včetně zobrazení průměrných hodnot bez nutného spuštění dotazu.
Systém umožňuje vizuálně porovnat současný průběh síťového provozu s historickými hodnotami. Porovnání probíhá pomocí časového intervalu, který lze flexibilně volit. Systém vypočítává procentuální změny pro jednotlivé časové intervaly a graficky vizualizuje nárůst nebo pokles síťového provozu.	Vizualizace historických trendů síťového provozu	ANO / Řešení umožňuje vizualizaci historických trendů síťového provozu s možností flexibilní volby časového intervalu.
Generování statistik a podrobných výpisů nad volitelnými časovými intervaly s volitelnými filtry. Různé formáty výstupů, minimálně PDF, CSV.	Analýza dat a ad hoc výstupy	ANO / Řešení umožňuje generování statistik a výpisů nad volitelnými časovými intervaly a s filtry a výstupy dle potřeb uživatele.

Systém umožňuje zpracovávat dotazy na dlouhé časové intervaly s délkou minimálně 1 měsíc bez nutnosti dotaz rozdělit dotaz na menší časové intervaly. Spuštění a vykonání dotazu není limitováno délkou časového intervalu nebo maximální dobou vykonávání dotazu. Dotazy, které se vykonávají dlouho, běží na pozadí a výsledky si uživatel může prohlídnout, jakmile je dotaz dokončen a výsledky jsou dostupné.	Analýza dat pomocí dotazů na dlouhé časové intervaly	ANO / Nabízené řešení umožňuje zpracovávat dotazy na dlouhé časové intervaly v jednom kroku.
Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Koláčové i průběhové grafy. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF nebo CSV. Automatická distribuce reportů e-mailem. Možnost automatického ukládání reportů na externí síťové úložiště.	Reporting	ANO / Řešení zahrnuje předdefinovanou sadu reportů, které lze uživatelsky konfigurovat. Reporty jsou dostupné v uvedených formátech, koláčové i průběhové, lze je ukládat na externí úložiště.
Řízení uživatelského přístupu k jednotlivým typům reportů (uživatel je oprávněn zobrazovat pouze statistiky, ke kterým mu bylo nastaveno oprávnění administrátorem).	Řízení uživatelského přístupu	ANO / Řešení umožňuje řízení přístupových oprávnění k jednotlivým reportům.
Výpis tzv. top N statistiky podle různých kritérií (počet přenesených bajtů, paketů, toků, nejvyšší hodnoty RTT, průměrné hodnoty SRT, atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu.	Top N statistiky	ANO / Řešení umožňuje výpis Top N statistik dle uvedených parametrů.
Systém umožňuje filtrovat s využitím libovolných atributů flow statistik vč. L7 rozšíření nebo výkonnostních parametrů sítě. Filtry je možné kombinovat prostřednictvím logických spojek AND, OR, NOT. Výstupy je možné formátovat, zejména zahrnout do zobrazení jednotlivé atributy flow záznamů nebo používat řazení	Filtrování a přizpůsobení výstupů	ANO / Řešení umožňuje filtrovat dle uvedených atributů a kombinací logických spojek, výstupy lze formátovat dle požadovaných parametrů.

(např. dle objemu přenesených dat, dle času nebo dle výkonnostních parametrů datové komunikace).		
Automatická notifikace v případě vzniku uživatelem definované situace (např. nadměrný přenos dat, překročení definované relativní nebo absolutní prahové hodnoty, atd.) prostřednictví emailu, SNMP trapu a syslogu, možnost automatického spuštění uživatelem definovaného skriptu.	Uživatelsky definovatelné alerty	ANO / Řešení umožňuje uživatelsky definované notifikace dle uvedených parametrů.
Uživateli je umožněno definovat si vlastní perzistentní pohledy na data, které budou systémem kontinuálně aktualizovány. K definici pohledu je možné použít libovolný filtr (komunikace daného síťového segmentu, download a upload na server podnikové aplikace, protokol HTTP, apod.).	Uživatelsky definované pohledy na datový provoz	ANO / Řešení umožňuje vlastní uživatelsky definované, kontinuálně altualizovaní perzistentní pohledy na data prostřednictvím libovolného filtru.
Možnost dohledat každý jednotlivý datový tok (flow záznam).	Drill-down	ANO / Řešení umožňuje dohleda každý jednotlivý datový tok.
Systém umožňuje vizualizovat využití sítě v geografickém nebo logickém kontextu pomocí síťové topologie.	Síťová topologie	ANO / Řešení umožňuje vizualizovat využití sítě v geografickém nebo logickém kontextu prostřednictvím síťové topologie.
Monitorování zařízení připojených k datové síti, dlouhodobá historie aktivních zařízení, identifikace na základě IP adresy, MAC adresy, sledování VLAN, operačního systému, přihlášeného uživatele na daném zařízení.	Monitoring aktivních zařízení na síti	ANO / Řešení monitoruje zařízení připojená k datové síti, jejich dlouhodobou historii, identifikuje je prostřednictvím uvedených parametrů.

Systém automaticky obohacuje přijímané flow statistiky na základě IP adresy. Provoz je možné filtrovat na základě dané geografické lokality (státu/země).	Automatická podpora geolokace	ANO / Řešení automaticky obohacuje flow statistiky na základě IP adresy a umožňuje filtrovat provoz na základě geografické lokality.
Kolektor poskytuje veřejně dokumentované API pro získávání a zpracování dat. Prostřednictvím API je možné kolektor rovněž konfigurovat (např. definovat vlastní pohledy, reporty, apod.).	Otevřené rozhraní	ANO / Řešení poskytuje veřejně dokumentované API pro získávání a zpracování dat, jehož prostřednictvím lze kolektor konfigurovat.
Monitorování dostupnosti zdroje flow dat pomocí SNMP.	Monitorování dostupnosti zdroje flow dat	ANO / Řešení monitoruje dostupnost zdroje flow dat přes SNMP.
Požadavky na automatické vyhodnocování NetFlow dat		
Minimální technické požadavky	Technický parametr	Popis splnění požadavku
Podpora standardů NetFlow v5, NetFlow v9, IPFIX, jFlow, cflowd, NetStream. Podpora VPC flow logů z AWS, Azure a GCP.	Podpora flow standardů	ANO / Řešení podporuje uvedené standardy.
Architektura systému umožňuje streamové zpracovávání flow dat pro rychlou detekci bezpečnostních nebo provozních anomálií.	Streamové zpracovávání flow dat	ANO /Architektura řešení umožňuje streamové zpracování flow dat.
Systém detekce anomálií poskytuje veřejně dokumentované API pro získávání a zpracování událostí. Prostřednictvím API je možné systém detekce anomálií rovněž konfigurovat (např. vytvářet filtry, měnit nastavení detekčních metod, apod.).	Otevřené rozhraní	ANO / Řešení poskytuje veřejně dokumentované API pro získání a zpracování událostí, jehož prostřednictvím jej lze konfigurovat.
Systém umožňuje postupné rozšiřování řešení pro automatické vyhodnocení přidáním dalších instancí systému při zachování jednoho uživatelského rozhraní pro dané řešení bez ohledu na počet zapojených instancí.	Škálovatelnost řešení	ANO / Řešení umožňuje škálování a postupné rozšiřování pro připojení dalších instancí při zachování jednoho GUI.
Systém umožňuje deduplikovat flow statistiky před jejich vlastní analýzou.	Deduplikace	ANO / Řešení umožňuje deduplikovat flow statistiky před provedením jejich analýzy.

Systém umožňuje korelovat toky před a za proxy serverem před jejich vlastní analýzou s cílem identifikovat provoz procházející proxy serverem a tento provoz přiřadit koncovému uživateli.	Proxy korelace	ANO / Řešení umožňuje korelovat toky před a za proxy serverem před provedením analýzy.
Systém podporuje vzorkování na úrovní toků před jejich vlastním zpracováním.	Vzorkování na úrovni toků	ANO / Řešení podporuje vzorkování na úrovni toků.
Systém umožňuje spravovat zdroje síťových toků, umožňuje dočasně pozastavit příjem toků a indikovat poruchu zdroje síťových toků.	Správa zdrojů síťových toků	ANO / Řešení umožňuje spravovat zdroje síťových toků, dočasně je pozastavit a indikovat poruchu zdroje.
Systém zobrazuje informace o identitě uživatelů obsaženou ve flow datech jako součást události.	Identita uživatelů	ANO / Řešení umožňuje zobrazovat informace o identitě uživatelů obsaženou ve flow datech jako součást události.
Systém obsahuje vestavěnou databázi nejčastěji používaných SaaS aplikací a platforem na Internetu (1000 a více). Informace z databáze jsou používány k mapování aplikací na externí IP adresy. Informace o SaaS aplikacích a platformách je prezentována v UI u externích IP adres, pro které mapování existuje.	Mapování aplikací k IP adresám	ANO / Řešení obsahuje databázi SaaS aplikací a platforem na Internetu, která je používaná k mapování aplikací z externí IP adresy.
Systém podporuje persistenci doménových jmen, tedy uložení doménové jména původce události v okamžiku zaznamenání výskytu této události.	Persistence doménových jmen	ANO / Řešení podporuje persistenci doménových jmen.
Systém obsahuje předdefinovanou sadu detekčních metod a algoritmů pro analýzu flow statistik, detekci bezpečnostních incidentů, provozních problémů a síťových anomálií. Tyto metody detekují bezpečnostní události bez potřeby signatur.	Detekční pravidla a algoritmy nevyžadující signatury	ANO / Řešení obsahuje předdefinovanou sadu detekčních pravidel pro analýzu a detekci bezpečnostních a provozních událostí a anomálií.

Systém sbírá, ukládá a vizualizuje události z nástroje třetí strany - Suricata IDS. Události detekované na základě signatur pomocí Suricata IDS jsou korelovány s událostmi detekovanými pravidly a algoritmy nevyžadující signatury.	Analýza a korelace událostí detekovaných na základě signatur	ANO / Řešení zpracovává a vizualizuje události na základě signatur a tyto jsou korelovány s událostmi detekovanými pravidly bez signatur..
Aktivita zařízení v síti je vyhodnocována a skórována číselným indexem, který umožňuje jednoduše identifikovat nejzávažnější zařízení z pohledu bezpečnostních hrozeb. Systém poskytuje pohled na zařízení seřazený podle indexu rizika.	Hodnocení zařízení mírou rizika	ANO / Řešení vyhodnocuje a skóruje aktivity v síti číselným indexem pro jednoduchou identifikaci nejzávažnějších událostí a umožňuje řadit zařízení dle indexu rizika.
Systém poskytuje shrnující přehled, který obsahuje nejzávažnější bezpečnostní události a síťové zařízení, nově detekované hrozby a významné změny v monitorované síti z pohledu bezpečnosti. Toto shrnutí zjednodušuje prioritizaci práce bezpečnostního analytika.	Shrnutí bezpečnostní situace	ANO / Řešení poskytuje přehled nejzávažnějších událostí a síťových zařízení, nově detekované události a změny v síti z pohledu bezpečnosti.
Detekce skenování portů, slovníkové útoky, útoky odepření služeb (DoS), útoky na síťové protokoly SSH, RDP, Telnet a další obdobné služby.	Detekce síťových útoků	ANO / Řešení detekuje všechny uvedené metody rizikových aktivit a útoků v síti.
Detekce anomálií v DNS, DHCP, SMTP, multicast provozu a nestandardní komunikace.	Detekce anomálií v síťovém provozu	ANO / Řešení detekuje uvedené anomálie a nestandardní komunikaci.
Detekce NATů v síti s využitím rozšířených informací z L3/L4.	Detekce NATů	ANO / Řešení detekuje NATy v síti.
Detekce P2P sítí a VPN komunikace.	Detekce nežádoucích aplikací	ANO / Řešení detekuje P2P sítě a VPN komunikaci.
Systém detekuje komunikace s různými SaaS aplikacemi a platformami (1000+) patřících do různých kategorií. Seznam SaaS aplikací a platforem je automaticky poskytován a aktualizován výrobcem. Uživatel si může libovolně vybrat, s jakými	Blacklistování aplikací	ANO / Řešení detekuje komunikaci s uvedenýcmi typy aplikací, podporuje aktualizaci seznamu a uživatelské přizpůsobení seznamu nežádoucí komunikace a typ

aplikacemi bude komunikace detekována a reportována jako událost.		reportování takových komunikací.
Systém umožňuje detekovat závadnou komunikací na základě rozlišení legitimních domén (druhé úrovně) od náhodně generovaných domén.	Detekce náhodných domén	ANO / Řešení umožňuje detekci závadné komunikace na základě náhodně generovaných domén.
Systém umožňuje detekovat DNS přes HTTPS (DoH) komunikace a použití DoH serverů.	Detekce DNS přes HTTPS (DoH) komunikací	ANO / Řešení umožňuje detekování DNS přes HTTPS.
Detekce použití TOR klientů v monitorované síti a detekce příchozí komunikace z TOR sítě na monitorované servery.	Detekce TOR komunikace	ANO / Řešení detekuje použití TOR komunikace.
Systém umožňuje detekovat závadné komunikace monitorování JA3 otisků v síťovém provozu a jejich porovnáváním se seznamem známých závadných JA3 otisků.	Analýza šifrovaného provozu použitím JA3 otisků	ANO / Řešení umožňuje detekci závadné komunikace monitorování JA3 otisků v síti prostřednictvím porovnání se seznamem známých závadných JA3 otisků.
Systém umožňuje identifikovat bezpečnostní události (např. komunikaci s botnet command & control centry, přístup na phishing servery, apod.) využíváním zdrojů IP a host reputačních databází poskytovaných výrobcem a aktualizovaných nejméně každých 24 hodin. Systém umožňuje zapojit další zdroje IP a host reputačních dat pro automatickou detekci.	Detekce událostí na základě „Threat intelligence“ dat	ANO / Řešení umožňuje detekci bezpečnostních událostí na základě využití threat intelligence, reputační databáze je aktualizovaná častěji než každých 24 hodin (obvykle na hodinové bázi); umožňuje využít další zdroje IP a reputačních dat.
Systém lze napojit na MISP platformu a použít indikátory kompromitace (IoC) poskytované touto platformou k detekci závadných komunikací v monitorované síti.	Podpora MISP platformy	ANO / Řešení umožňuje napojení na MISP platformu a využití IoC poskytované k detekci závadné komunikace.

Detekce nadměrné zátěže sítě, výpadků služeb,, nových a cizích zařízení připojených k síti.	Detekce provozních problémů	ANO / Řešení umožňuje detekci uvedených provozních problémů monitorované sítě.
Detekce síťových anomálií na základě predikce budoucího chování sítě s využíváním znalosti historie komunikace.	Detekce síťových anomálií	ANO / Řešení detekuej síťové anomálie na základě predikce budoucího chování sítě využitím znalosti historie komunikace.
Systém umožňuje definovat vlastní detekční metody pomocí poskytnutých příkazů, které vyhledávají ve flow statistikách (včetně informací z aplikační vrstvy) specifické vzory chování. Události detekované vlastními metodami jsou zpracovávány standardně jako události z dostupných detekčních metod (notifikace, reportování, atd.).	Definice vlastních detekčních metod	ANO / Řešení umožňuje definici vlastních detekčních metod pomocí příkazů, přičemž tyto jsou standardně zpracovány jako ostatní události dle jiných metod.
Systém je schopen k jednotlivým detekcím vytvářet a evidovat události a umožňuje jejich analýzu v uživatelském prostředí.	Vytváření událostí	ANO / Řešení umožňuje vytvářet a evidovat události k jednotlivým detekcím a analyzovat je v GUI.
Systém nabízí flexibilní uživatelské rozhraní pro vyhledávání událostí dle různých parametrů (typ události, IP adrese původce události, filtr, přiřazení události do kategorie, ID události apod.). Události je možné prezentovat různým způsobem (prostý seznam, agregace dle zdrojů, dle cílů apod.).	Vyhledávání událostí	ANO / Řešení poskytuje flexibilní GUI pro vyhledávání událostí dle uvedených parametrů a nejrůznější formy jejich prezentování.
Systém je schopen poskytnout přímý přístup k evidované události za pomoci ID události z externích systémů za pomoci unikátního URL, které je možné sestavit v externím systému při znalosti ID události.	Přímý přístup k události přes unikátní URL s využitím ID události	ANO / Řešení poskytuje přímý přístup k události přes unikátní URL s využitím ID události.

Systém umožňuje interaktivní vizualizaci detekovaných událostí formou grafické reprezentace flow statistik, na základě kterých byla událost rozpoznána.	Interaktivní vizualizace událostí	ANO / Řešení umožňuje interaktivní vizualizaci detekovaných událostí formou grafické prezentace flow dat, na jejichž základě události vznikly.
Systém integruje informace ze služeb DNS, WHOIS, geolokační služby. Uživatelsky definované externí služby fungující na protokolu HTTP/HTTPS.	Integrace informací z jiných služeb	ANO / Řešení integruje informace z uvedených služeb.
Systém je schopen za pomoci zabezpečeného komunikačního rozhraní získat další informace k IP adrese z adresářových služeb AD/LDAP.	Získávání doplňujících informací z adresářových služeb	ANO / Řešení umožňuje získat informace k IP adrese z uvedených adresářových služeb pomocí zabezpečeného komunikačního rozhraní.
Události je možné přiřazovat do uživatelsky definovaných kategorií (např. vyřešeno, důležité, apod.). Událostem je možné přímo v systému pořizovat poznámky a komentáře.	Kategorie a komentáře	ANO / Řešení umožňuje přiřazení událostí do uživatelsky definovaných kategorií a přiřazovat k nim poznámky a komentáře přímo v systému.
Detekované události jsou mapovány na jednu nebo více MITRE ATT&CK taktik a technik pro poskytnutí širšího kontextu uživateli. Mapování je založeno na základě kontextové analýzy pro zajištění správného mapování taktiky a techniky na detekovanou událost. Stejný druh události tak může být mapován různě v závislosti na kontextu události nebo vývoji události v čase.	Podpora MITRE ATT&CK frameworku a mapování na základě kontextu	ANO / Řešení umožňuje mapovat detekované události na MITRE ATT&CK taktiky a techniky na základě kontextu.
Systém poskytuje dashboard pro vizualizaci MITRE ATT&CK matice, která zobrazuje počet událostí detekovaných v jednotlivých taktikách a technikách čímž umožňuje poskytnout přehled nad stávající bezpečností situací a zobrazit útoky v jejich různých fázích dle MITRE ATT&CK frameworku.	MITRE ATT&CK dashboard a vizualizace	ANO / Řešení poskytuje dashboard pro vizualizaci MITRE ATT&CK matice a zobrazit útoky v různých fázích dle tohoto frameworku.

Systém obsahuje konfiguračního průvodce pro nastavení systému při prvním spuštění podle parametrů sítě, do kterého je systém nasazen.	Konfigurační průvodce	ANO / Řešení obsahuje konfiguračního průvodce pro nastavení dle parametrů sítě.
Jednotlivé detekční schopnosti je možné konfigurovat a parametrizovat tak, aby bylo dosaženo maximální efektivity a minimálního počtu falešných poplachů. Detekční mechanismy je možné konfigurovat různým způsobem (např. s různou citlivostí) pro statistiky z různých segmentů sítě (např. LAN nebo DMZ).	Konfigurace detekčních schopností	ANO / Řešení umožňuje konfigurovat a parametrizovat jednotlivé detekční schopnosti pro minimalizaci falešných poplachů, různým způsobem pro jednotlivé segmenty sítě.
Předdefinované priority událostí s možností uživatelského nastavení závažnosti událostí na základě IP adresních rozsahů, typů událostí, míst výskytu nebo detailů události. Jedna událost může mít v závislosti na konfiguraci přiřazeno více priorit.	Definice závažnosti událostí	ANO / Řešení zahrnuje předdefinované priority událostí a umožňuje uživatelské nastavení, přičemž priority události se mohou lišit dle konfigurace.
Systém umožňuje spravovat detekční metody z uživatelského prostředí, vytvářet kopie detekčních metod a nastavit jejich individuální parametry.	Správa detekčních metod	ANO / Řešení umožňuje správu detekčních metod z GUI, stejně jako kopírovat detekční metody a nastavovat jejich individuální parametry.
Systém umožňuje předdefinovat uživatelské pohledy na události a prioritu dle uživatelských rolí.	Různé pohledy na události podle uživatelských rolí	ANO / Řešení umožňuje předdefinovat uživatelské pohledy na události a priority dle rolí.
Systém umožňuje definovat filtry vč. komplexních filtrů složených z dílčích filtrů. Pro zjednodušení definice filtrů je možné používat operace jako inverze nebo rozdíl filtrů. Filtry je možné exportovat do formátu XML nebo z tohoto formátu importovat. K jednotlivým záznamům a filtrům lze připojit uživatelský popis účelu.	Správa filtrů	ANO / Řešení umožňuje definovat komplexní filtry, tyto exportovat a importovat a připojovat k nim uživatelský popis.

Případné události, které představují falešné poplachy (false positives) je možné odstranit prostřednictvím jednoduché konfigurace pravidel pro vyloučení falešných poplachů dostupné v uživatelském rozhraní.	Správa falešných poplachů	ANO / Řešení umožňuje odstranit falešně pozitivní události pomocí jednoduché konfigurace pravidel v GUI.
Systém umožňuje zastavit a opět spustit pravidla falešného poplachu, aby bylo možné ověřit jejich požadovanou funkčnost při běžném provozu.	Pozastavení platnosti pravidla falešných poplachů	ANO / Řešení umožňuje zastavit a opět spusti falešně pozitivní pravidla s cílem ověření jejich funkčnosti.
Pro definici falešných poplachů lze využít filtrů které mohou být upravovány nezávisle na dané definici pravidla falešného poplachu.	Dynamické definice falešných poplachů	ANO / Řešení umožňuje využít filtry pro definici falešných poplachů a upravit je nezávisle na definici takového pravidla.
Pravidla pro falešné poplachy je možné definovat pomocí čísel autonomních systémů (ASN) nebo pomocí plně kvalifikovaného doménového jména (FQDN), čímž lze označit provoz, který nebude zpracováván detekčními metodami.	Definice falešných poplachů pomocí ASN a FQDN	ANO / Řešení umožňuje definovat pravidla pro falešné poplachy pomocí ASN a FQDN.
Systém loguje veškeré změny konfigurace s cílem zajistit auditovatelnost činnosti uživatelů a provedené změny s dopadem detekci událostí. Změny konfigurace je možné rovněž odesílat protokolem syslog pro auditování formou externího systému typu SIEM nebo log management.	Sledování změn konfigurace	ANO / Řešení loguje změny konfigurace pro audit činnosti uživatelů; změny konfigurace umožňuje odesílat do externího systému.
Události je možné automaticky exportovat ve formátu CEF protokolem Syslog. Předpokládané využití této funkcionality je integrace se systémy typu SIEM nebo log management. Součástí exportu musí být event ID, které jednoznačně identifikuje danou událost.	CEF export	ANO / Řešení umožňuje automatický export událostí v uvedeném formátu a integraci se systémy SIEM a log management.
Události je možné reportovat do dohledových systémů	SNMP Trap	ANO / Řešení umožňuje report událostí do

prostřednictvím funkcionality SNMP trap.		dohledových systémů přes SNMP trap.
Události je možné exportovat do formátu CSV pro další zpracování.	CSV export	ANO / Řešení umožňuje export událostí do CSV.
Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF. Automatická distribuce reportů e-mailem.	Reporting	ANO / Řešení obsahuje předdefinovanou sadu reportů, které lze uživatelsky konfigurovat, automaticky distribuovat e-mailem a získat ve webovém GUI v PDF.
Notifikace o detekovaných událostech prostřednictvím e-mailu s podporou různých formátů (HTML, incident handling systém, úsporný textový formát). Možnost připojit vzorek flow dat, na základě kterých byla událost detekována k e-mailovému reportu.	E-mailové notifikace	ANO / Řešení umožňuje notifikaci o detekovaných událostech uvedenými způsoby.
Na výskytu události je možné automaticky reagovat spuštěním záchytu provozu v plném rozsahu. Tyto záchyty je možné uživatelsky spravovat.	Záchyt provozu v plném rozsahu	ANO / Řešení umožňuje automaticky reagovat na výskyt události spuštěním záchytu provozu, což lze uživatelsky spravovat.
Na výskyt události je možné automaticky reagovat spuštěním uživatelsky definovaných skriptů.	Spuštění skriptu	ANO / Řešení umožňuje automatickou reakci na výskyt události spuštěním uživatelsky definovaných scriptů.

Nástroj pro ověřování identity uživatelů		
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
nastavení	ANO	nastavení
akceptační testy a testovací provoz	ANO	akceptační testy a testovací provoz
školení administrátorů v rozsahu 4 hodin	ANO	školení administrátorů v rozsahu 4 hodin
dokumentace skutečného provedení	ANO	dokumentace skutečného provedení

ID005 - MFA + SSO ochrana identity uživatelů

Nasazení MFA + SSO je v rámci IS posílení Kybernetické ochrany. Uživatelům bude řešení umožňovat používání různých autentizačních předmětů pro více-faktorovou autentizaci. Řešení bude také poskytovat funkci automatického přihlášení SSO (Single Sign-On) do všech IS ve škole používaných.

Nasazení MFA jednoznačně posiluje bezpečnost provozovaného IS a nasazení SSO jednoznačně zrychluje a zefektivňuje uživatelskou práci s IS.

Nástroj pro ověřování identity uživatelů		
Název a výrobce	**Výrobce: Gitrix** **Název: GITRIX**	
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
Funkční požadavky na systém		
Systém musí být koncipován pro provoz a licenčně pokrýt minimálně 1000 uživatelů (tzn. umožní .přiřadit minimálně 1000 uživatelům autentizační prostředky (neomezené množství) a spravovat digitální certifikáty(neomezené množství)).	ANO	Systém musí být koncipován pro provoz a licenčně pokrýt minimálně 1000 uživatelů (tzn. umožní .přiřadit minimálně 1000 uživatelům autentizační prostředky (neomezené množství) a spravovat digitální certifikáty(neomezené množství)).

Systém zajistí, že vydávání interních certifikátů (X.509) i od akreditovaných CA (komerční, kvalifikované) bude zajištěn ve stejném uživatelském rozhraní, v rámci jednotného procesu a analogických funkcionalit v rámci zajištění správy jejich životního cyklu (následná obnova, revokace, atd.), stejně tak jako další druhy certifikátů, aby Zadavatel mohl systém využívat a provozovat pomocí méně kvalifikovaných zaměstnanců s menšími nároky na školení a úroveň dosaženého vzdělání.	ANO	Systém zajistí, že vydávání interních certifikátů (X.509) i od akreditovaných CA (komerční, kvalifikované) bude zajištěn ve stejném uživatelském rozhraní, v rámci jednotného procesu a analogických funkcionalit v rámci zajištění správy jejich životního cyklu (následná obnova, revokace, atd.), stejně tak jako další druhy certifikátů, aby Zadavatel mohl systém využívat a provozovat pomocí méně kvalifikovaných zaměstnanců s menšími nároky na školení a úroveň dosaženého vzdělání.
Systém zajistí plnou správu PUK / Management key (dále klíč) pro tokeny zabezpečeným způsobem. Tyto kódy se nesmí tisknout a nejsou dostupné žádné osobě (viditelně). Systém tento klíč zabezpečeným způsobem eviduje a umožní jeho čtení pouze uživateli pomocí vlastní karty pro příslušné operace (s de-šifrovaným klíčem pracuje pouze daná aplikace pro vykonání práce s tokenem). Např: šifrováno klíčem na daném tokenu, klíč uložen v centrální databázi systému (bez tokenu nelze přečíst).	ANO	Systém zajistí plnou správu PUK / Management key (dále klíč) pro tokeny zabezpečeným způsobem. Tyto kódy se nesmí tisknout a nejsou dostupné žádné osobě (viditelně). Systém tento klíč zabezpečeným způsobem eviduje a umožní jeho čtení pouze uživateli pomocí vlastní karty pro příslušné operace (s de-šifrovaným klíčem pracuje pouze daná aplikace pro vykonání práce s tokenem). Např: šifrováno klíčem na daném tokenu, klíč uložen v centrální databázi systému (bez tokenu nelze přečíst).

Systém je provozovatelný na systémech založených na open source (bez nutnosti kupovat licence): Operační systém, Databázový systém a případně další vrstvy systému.	ANO	Systém je provozovatelný na systémech založených na open source (bez nutnosti kupovat licence): Operační systém, Databázový systém a případně další vrstvy systému.
Systém zajistí kompatibilitu s oficiálními ovladači karet / tokenů bez nutnosti instalovat jiný SAC / Middleware vyráběný jinou stranou než výrobce.	ANO	Systém zajistí kompatibilitu s oficiálními ovladači karet / tokenů bez nutnosti instalovat jiný SAC / Middleware vyráběný jinou stranou než výrobce.
Systém umožní pomoc uživatelům s uzamčeným čipem pomocí šifrovaném PUKU bez nutnosti asistence jiné osoby s vyšším delegovaným oprávněním.	ANO	Systém umožní pomoc uživatelům s uzamčeným čipem pomocí šifrovaném PUKU bez nutnosti asistence jiné osoby s vyšším delegovaným oprávněním.
Systém umožní uživateli změnu PIN bez nutnosti asistence jiné osoby s vyšším delegovaným oprávněním.	ANO	Systém umožní uživateli změnu PIN bez nutnosti asistence jiné osoby s vyšším delegovaným oprávněním.
Systém umožní uživateli resetovat zapomenutý nebo uzamčený PIN pro svoji kartu samoobslužným procesem bez nutnosti asistence jiné osoby s vyšším delegovaným oprávněním.. Tento proces nejdříve ověří identitu uživatele před tím, než mu bude umožněno nastavení nového PINu. Ověření bude provedeno na základě e-mailu zaslaného ze systému. Email obsahuje bezpečný link pro ověření identity uživatele a následně dojde k dešifrování PUKu pro účely změny PIN / odblokování (uživatel PUK nevidí)	ANO	Systém umožní uživateli resetovat zapomenutý nebo uzamčený PIN pro svoji kartu samoobslužným procesem bez nutnosti asistence jiné osoby s vyšším delegovaným oprávněním.. Tento proces nejdříve ověří identitu uživatele před tím, než mu bude umožněno nastavení nového PINu. Ověření bude provedeno na základě e-mailu zaslaného ze systému. Email obsahuje bezpečný link

		pro ověření identity uživatele a následně dojde k dešifrování PUKu pro účely změny PIN / odblokování (uživatel PUK nevidí)
Workflow recyklace kvalifikovaného prostředku v systému obsahuje nejméně následující kroky: Systém musí vytvořit auditní záznam, že proběhla recyklace (recyklace automaticky obsahuje operace revokace certifikátů vydaných systémem a následné vymazání všech certifikátů a ostatních datových typů) na kvalifikovaném prostředku a byl nastaven nový defaultní PIN, PUK, digital signature PIN a PUK.	ANO	Workflow recyklace kvalifikovaného prostředku v systému obsahuje nejméně následující kroky: Systém musí vytvořit auditní záznam, že proběhla recyklace (recyklace automaticky obsahuje operace revokace certifikátů vydaných systémem a následné vymazání všech certifikátů a ostatních datových typů) na kvalifikovaném prostředku a byl nastaven nový defaultní PIN, PUK, digital signature PIN a PUK.
Systém musí uchovávat všechny informace o uživateli a jeho „přiřazené" čipové kartě tak, aby byl schopen je zprostředkovat dalším systémům v rámci možných integrací.	ANO	Systém musí uchovávat všechny informace o uživateli a jeho „přiřazené" čipové kartě tak, aby byl schopen je zprostředkovat dalším systémům v rámci možných integrací.
Systém musí obsahovat roli pro delegované osoby (například Operátor), která přiřazuje karty, vydává certifikáty a ověřuje identitu uživatelů. Přitom zajišťuje úkony spojené s vydáváním či správou životního cyklu kvalifikovaného prostředku pro uživatele.	ANO	Systém musí obsahovat roli pro delegované osoby (například Operátor), která přiřazuje karty, vydává certifikáty a ověřuje identitu uživatelů.

		Přitom zajišťuje úkony spojené s vydáváním či správou životního cyklu kvalifikovaného prostředku pro uživatele.
Operátor musí být osoba s důvěryhodným přístupem k systému. Pro operátora jako osobu vydávající platí stejná povinnost přihlášení k nástroji operátora prostřednictvím čipové karty.	ANO	Operátor musí být osoba s důvěryhodným přístupem k systému. Pro operátora jako osobu vydávající platí stejná povinnost přihlášení k nástroji operátora prostřednictvím čipové karty.
Operátor nemůže vydávat čipové karty uživatelům bez vlastního autentizačního prostředku zajišťujícího více-faktorovou autentizaci jeho osoby.	ANO	Operátor nemůže vydávat čipové karty uživatelům bez vlastního autentizačního prostředku zajišťujícího více-faktorovou autentizaci jeho osoby.
Systém musí obsahovat roli Administrátor, který spravuje celky jako: Správa administrátorů, správa uživatelů, správa serverů, správa skupin, zobrazení tokenů, auditního logu	ANO	Systém musí obsahovat roli Administrátor, který spravuje celky jako: Správa administrátorů, správa uživatelů, správa serverů, správa skupin, zobrazení tokenů, auditního logu
Systém musí logovat operace spojené se správou životního cyklu certifikátu a kvalifikovaného prostředku včetně identifikace provádějící osoby - dále jako auditní log. Tento auditní log je možné vidět ve webovém rozhraní v detailu uživatele, tokenu a nebo v globálním pohledu a to bez nutnosti technických znalostí.	ANO	Systém musí logovat operace spojené se správou životního cyklu certifikátu a kvalifikovaného prostředku včetně identifikace provádějící osoby - dále jako auditní log. Tento auditní log je možné vidět ve webovém rozhraní v detailu uživatele, tokenu a nebo v globálním pohledu a to bez nutnosti technických znalostí.

Systém zajistí podporu připojení dalších subjektů, přičemž jednotlivé subjekty musí být na sobě nezávislé a vzájemně nevidí na data ostatních subjektů, pokud k tomu nemají příslušné oprávnění a správu jednotlivých subjektů musí být možné delegovat na subjekty/uživatele nezávisle na sobě podle přidělených přístupových práv.	ANO	Systém zajistí podporu připojení dalších subjektů, přičemž jednotlivé subjekty musí být na sobě nezávislé a vzájemně nevidí na data ostatních subjektů, pokud k tomu nemají příslušné oprávnění a správu jednotlivých subjektů musí být možné delegovat na subjekty/uživatele nezávisle na sobě podle přidělených přístupových práv.
Notifikace systému musí být zasílány uživatelům (s možností nastavit notifikaci i operátorům) při blížící se expiraci certifikátu s možností nastavit časové limity při kterých se notifikace aplikují.	ANO	Notifikace systému musí být zasílány uživatelům (s možností nastavit notifikaci i operátorům) při blížící se expiraci certifikátu s možností nastavit časové limity při kterých se notifikace aplikují.
Systém bude kompatibilní se všemi typy zařízení (čipové karty/tokeny) u kterých jeho dodavatel poskytne součinnost.	ANO	Systém bude kompatibilní se všemi typy zařízení (čipové karty/tokeny) u kterých jeho dodavatel poskytne součinnost.
Systém je kompatibilní s QSCD prostředky jako např: Thales (Gemalto) čipové karty a usb tokeny, které z bezpečnostních důvodů umožňují nastavit hodnoty PUKu pro kvalifikovanou a nekvalifikovanou část samostatně.	ANO	Systém je kompatibilní s QSCD prostředky jako např: Thales (Gemalto) čipové karty a usb tokeny, které z bezpečnostních důvodů umožňují nastavit hodnoty PUKu pro kvalifikovanou a nekvalifikovanou část samostatně.
Systém musí obsahovat “Autoupdate službu” pro klientskou, operátorskou aplikaci a serververového agenta. Služba zajistí aktualizaci nových verzí (bez nutnosti zásahu administrátora).	ANO	Systém musí obsahovat “Autoupdate službu” pro klientskou, operátorskou aplikaci a serververového agenta. Služba zajistí aktualizaci nových verzí

		(bez nutnosti zásahu administrátora).
Systém umožní zneplatnění certifikátu (revokace, pro interní a kvalifikované certifikáty) a recyklaci karty v rámci jedné organizace a jednoho systému bez použití uživatelského rozhraní 3. stran.	ANO	Systém umožní zneplatnění certifikátu (revokace, pro interní a kvalifikované certifikáty) a recyklaci karty v rámci jedné organizace a jednoho systému bez použití uživatelského rozhraní 3. stran.
Systém umožní automatické obnovování certifikátů na PC uživatele bez zásahu (asistence) operátora. Operátor pouze schvaluje (povoluje) žádosti o obnovou. Samotná obnova musí proběhnout v režii uživatele pod jeho výhradní kontrolou v souladu s elDAS v rámci jednoho systému.	ANO	Systém umožní automatické obnovování certifikátů na PC uživatele bez zásahu (asistence) operátora. Operátor pouze schvaluje (povoluje) žádosti o obnovou. Samotná obnova musí proběhnout v režii uživatele pod jeho výhradní kontrolou v souladu s elDAS v rámci jednoho systému.
Systém umožní instalaci operátorské a klientské aplikace v podobě instalačních balíčků pro koncové zařízení (v podobě msi balíčku) a musí být podepsán CodeSignim certifikátem, který je akceptován Windows systémem. Dodavatel musí zajistit aktualizaci těchto aplikací v případě expirace aktuální verze znovu podepsat.	ANO	Systém umožní instalaci operátorské a klientské aplikace v podobě instalačních balíčků pro koncové zařízení (v podobě msi balíčku) a musí být podepsán CodeSignim certifikátem, který je akceptován Windows systémem. Dodavatel musí zajistit aktualizaci těchto aplikací v případě expirace aktuální verze znovu podepsat.

Systém obsahuje desktopové aplikace pro uživatele (klientská aplikace, pro automatické prodlužování, pomoc s PIN / tokenem) a operátora (vydávání certifikátů, přiřazování tokenů). Aplikace musí běžet na Windows 10/11.	ANO	Systém obsahuje desktopové aplikace pro uživatele (klientská aplikace, pro automatické prodlužování, pomoc s PIN / tokenem) a operátora (vydávání certifikátů, přiřazování tokenů). Aplikace musí běžet na Windows 10/11.
Systém umožní vydání karty, vydání balíčku certifikátů (kvalifikovaný a komerční) v rámci Online napojení na CA v jednom systému bez použití uživatelského rozhraní 3. stran.	ANO	Systém umožní vydání karty, vydání balíčku certifikátů (kvalifikovaný a komerční) v rámci Online napojení na CA v jednom systému bez použití uživatelského rozhraní 3. stran.
Požadavek na proces vydávání kvalifikovaných certifikátů mimo pracovní dobu. Proces vydání kvalifikovaného certifikátu by měl být zajištěn tak, aby byl dostupný v kterékoli době, ať už jde o standardní pracovní dobu úřadu nebo certifikační autority. Je klíčové, aby proces probíhal bez zbytečných prodlev, zajišťující kontinuitu služby a efektivitu řešení výdejů certifikátů. Pro efektivní realizaci tohoto požadavku je důležité využít automatizované procesy, které eliminují potřebu časově omezeného lidského schvalování, zatímco zůstanou zachovány všechny bezpečnostní a legislativní standardy. Tímto způsobem bude garantována dostupnost služby i v mimořádných časech a situacích.	ANO	Požadavek na proces vydávání kvalifikovaných certifikátů mimo pracovní dobu. Proces vydání kvalifikovaného certifikátu by měl být zajištěn tak, aby byl dostupný v kterékoli době, ať už jde o standardní pracovní dobu úřadu nebo certifikační autority. Je klíčové, aby proces probíhal bez zbytečných prodlev, zajišťující kontinuitu služby a efektivitu řešení výdejů certifikátů. Pro efektivní realizaci tohoto požadavku je důležité využít automatizované procesy, které eliminují potřebu časově omezeného lidského schvalování, zatímco zůstanou zachovány všechny bezpečnostní a legislativní standardy. Tímto způsobem bude

		garantována dostupnost služby i v mimořádných časech a situacích.
Celý životní cyklus kvalifikovaného prostředku musí být spravován v rámci systému. Organizace nesmí být nucena posílat kvalifikované prostředky fyzicky do prostoru třetích stran.	ANO	Celý životní cyklus kvalifikovaného prostředku musí být spravován v rámci systému. Organizace nesmí být nucena posílat kvalifikované prostředky fyzicky do prostoru třetích stran.
V rámci recyklace nesmí opustit kvalifikovaný prostředek prostředí organizace, být zasílán třetím stranám, případně používat pro účely recyklace PIN čipové karty.	ANO	V rámci recyklace nesmí opustit kvalifikovaný prostředek prostředí organizace, být zasílán třetím stranám, případně používat pro účely recyklace PIN čipové karty.
Reporting systému musí umožňovat generovat automaticky měsíční reporty obsahující minimálně předávací protokoly dle jednotlivých subjektů převzetí smluvní dokumentace CA, počty vydaných certifikátů dle subjektů a operátorů, počty revokovaných certifikátů dle subjektů a operátorů, počet uživatelů systému CMS dle subjektů.	ANO	Reporting systému musí umožňovat generovat automaticky měsíční reporty obsahující minimálně předávací protokoly dle jednotlivých subjektů převzetí smluvní dokumentace CA, počty vydaných certifikátů dle subjektů a operátorů, počty revokovaných certifikátů dle subjektů a

		operátorů, počet uživatelů systému CMS dle subjektů.
Systém musí být připraven a umožnit v případě potřeby vydání balíčku certifikátů (kvalifikovaný a komerční) přímým online napojením minimálně alespoň dvě akreditované CA, aby měl zákazník možnost v případě nespokojenosti a přechod na jinou CA:	ANO	Systém musí být připraven a umožnit v případě potřeby vydání balíčku certifikátů (kvalifikovaný a komerční) přímým online napojením minimálně alespoň dvě akreditované CA, aby měl zákazník možnost v případě nespokojenosti a přechod na jinou CA:
- eIdentity	ANO	- eIdentity
- I.CA	ANO	- I.CA
Systém musí obsahovat integraci na Active Directory pro napojení a to zabezpečeným způsobem (SSL komunikace, možnost běhu vrstvy mimo v jiné síti než běží samotný systém) a to s podporou připojení AD na úrovni subjektů (každý subjekt v systému může mít vlastní AD).	ANO	Systém musí obsahovat integraci na Active Directory pro napojení a to zabezpečeným způsobem (SSL komunikace, možnost běhu vrstvy mimo v jiné síti než běží samotný systém) a to s podporou připojení AD na úrovni subjektů (každý subjekt v systému může mít vlastní AD).

Integrace synchronizace uživatelů z AD a jejich role, na základě které je dále řešen nárok na výdej obsahu na autentizační prostředek. Definice práv na základě členství v AD skupinách: Umožňuje přidělit oprávnění uživatelům a skupinám na základě jejich členství v AD DS. Delegování administrátorských oprávnění: Poskytuje možnost vytvářet různé kombinace oprávnění, které určují úrovně administrativního přístupu. Flexibilní delegování práv na konkrétní činnosti nebo nástroje. Automatická synchronizace identit: Zajišťuje, že identita uživatele v dodaném řešení odpovídá identitě v AD DS. Automatická synchronizace všech změn v AD DS (stav účtu, atributy, členství ve skupinách).	ANO	Integrace synchronizace uživatelů z AD a jejich role, na základě které je dále řešen nárok na výdej obsahu na autentizační prostředek. Definice práv na základě členství v AD skupinách: Umožňuje přidělit oprávnění uživatelům a skupinám na základě jejich členství v AD DS. Delegování administrátorských oprávnění: Poskytuje možnost vytvářet různé kombinace oprávnění, které určují úrovně administrativního přístupu. Flexibilní delegování práv na konkrétní činnosti nebo nástroje. Automatická synchronizace identit: Zajišťuje, že identita uživatele v dodaném řešení odpovídá identitě v AD DS. Automatická synchronizace všech změn v AD DS (stav účtu, atributy, členství ve skupinách).
Systém vydává interní certifikáty pomocí šablon certifikátů v Active Directory Certificates Service díky přímé integraci zabezpečeným způsobem (SSL komunikace, možnost běhu vrstvy mimo v jiné síti než běží samotný systém) v a to v jednoduchém uživatelském rozhraní pouze pověřeným uživatelům (verifikace uživatele pomocí certifikátu) ve stejné aplikaci jako kvalifikované certifikát. A to s podporou připojení AD CS na úrovni subjektů (každý subjekt v systému může mít vlastní AD CS).	ANO	Systém vydává interní certifikáty pomocí šablon certifikátů v Active Directory Certificates Service díky přímé integraci zabezpečeným způsobem (SSL komunikace, možnost běhu vrstvy mimo v jiné síti než běží samotný systém) v a to v jednoduchém

		uživatelském rozhraní pouze pověřeným uživatelům (verifikace uživatele pomocí certifikátu) ve stejné aplikaci jako kvalifikované certifikát. A to s podporou připojení AD CS na úrovni subjektů (každý subjekt v systému může mít vlastní AD CS).
Systém musí pomocí hybridních čipových karet nebo mobilní aplikace zajistit 2 faktorovou autentizaci uživatelů, tak aby byly naplněny podmínky ZoKB.	ANO	Systém musí pomocí hybridních čipových karet nebo mobilní aplikace zajistit 2 faktorovou autentizaci uživatelů, tak aby byly naplněny podmínky ZoKB.
Vícefaktorová (multifaktorová) autentizace (dále jen MFA) bude umožňovat Zadavateli využívat minimálně následující metody a kombinace faktorů:		Vícefaktorová (multifaktorová) autentizace (dále jen MFA) bude umožňovat Zadavateli využívat minimálně následující metody a kombinace faktorů:
Smartcard logon (kombinace přihlášení PIN+Certifikát X.509)	ANO	Smartcard logon (kombinace přihlášení PIN+Certifikát X.509)
Systém musí a bude umožňovat konfiguraci různých typů MFA, včetně biometrických metod a aplikací generujících kódy.	ANO	Systém musí a bude umožňovat konfiguraci různých typů MFA, včetně biometrických metod a aplikací generujících kódy.
Možnost nastavit přihlášení s následující kombinací faktorů pro vybrané uživatele (750 uživ.): Mobilní tel. (Mobilní aplikace) : VAR1: PUSH notifikace + Otisk prstu, VAR2: QR kód + TOTP (časově omezený)	ANO	Možnost nastavit přihlášení s následující kombinací faktorů pro vybrané uživatele (750 uživ.): Mobilní tel. (Mobilní aplikace) : VAR1: PUSH notifikace + Otisk prstu, VAR2: QR kód + TOTP (časově omezený)

Čipová karta musí umožňovat uložení certifikátu z interní certifikační autority založené na produktech Microsoft. Pomocí tohoto certifikátu se držitel karty bude moci přihlásit do doménových počítačů (technologie Smartcard Logon).	ANO	Čipová karta musí umožňovat uložení certifikátu z interní certifikační autority založené na produktech Microsoft. Pomocí tohoto certifikátu se držitel karty bude moci přihlásit do doménových počítačů (technologie Smartcard Logon).
Dodané kvalifikované prostředky - hybridní čipové karty budou v počtu 1000 ks s bezkontaktní částí typu: MifareDESFire 4K EV3	ANO	Dodané kvalifikované prostředky - hybridní čipové karty budou v počtu 1000 ks s bezkontaktní částí typu: MifareDESFire 4K EV3
K dodaným čipovým kartám je požadována dodávka kompatibilních čteček čipových karet v počtu 100 ks.	ANO	K dodaným čipovým kartám je požadována dodávka kompatibilních čteček čipových karet v počtu 100 ks.
K dodaným čipovým kartám je požadována dodávka USB klávesnic s rozložením kláves čeština, numerická klávesnice, barva černá, min. délka kabelu 1.6 m s kompatibilní čtečkou čipových karet v počtu 150 ks.	ANO	K dodaným čipovým kartám je požadována dodávka USB klávesnic s rozložením kláves čeština, numerická klávesnice, barva černá, min. délka kabelu 1.6 m s kompatibilní čtečkou čipových karet v počtu 150 ks.
Dodané hybridní čipové karty budou ve formátu ID-1 (velikost bankovní karty).	ANO	Dodané hybridní čipové karty budou ve formátu ID-1 (velikost bankovní karty).
Vlastnosti kontaktního čipu a PKI aplikace:		Vlastnosti kontaktního čipu a PKI aplikace:
· Všechny operace s privátním klíčem probíhají uvnitř čipu – klíč neopustí prostředí karty	ANO	· Všechny operace s privátním klíčem probíhají uvnitř čipu – klíč neopustí prostředí karty
· Privátní klíč uložený na kartě nelze z karty vyexportovat	ANO	· Privátní klíč uložený na kartě nelze z karty vyexportovat

· Vytváření kvalifikovaného elektronického podpisu splňující nařízení eIDAS na zařízení schválené ministerstvem vnitra	ANO	· Vytváření kvalifikovaného elektronického podpisu splňující nařízení eIDAS na zařízení schválené ministerstvem vnitra
· Klíče pro kvalifikovaný elektronický podpis jsou generovány v čipu.	ANO	· Klíče pro kvalifikovaný elektronický podpis jsou generovány v čipu.
· Klíče, které nejsou určeny pro kvalifikovaný elektronický podpis, mohou být generovány v čipu a nebo mohou být na kartu importovány	ANO	· Klíče, které nejsou určeny pro kvalifikovaný elektronický podpis, mohou být generovány v čipu a nebo mohou být na kartu importovány
· Generování RSA i ECC klíčů v čipu i import klíčů s certifikáty do čipu, ze souboru formátu PKCS#12	ANO	· Generování RSA i ECC klíčů v čipu i import klíčů s certifikáty do čipu, ze souboru formátu PKCS#12
Podporované jsou minimálně kryptografické algoritmy:		Podporované jsou minimálně kryptografické algoritmy:
· Symetrické: 3DES, AES	ANO	· Symetrické: 3DES, AES
· Hash: SHA-1, SHA-256, SHA-384, SHA-512.	ANO	· Hash: SHA-1, SHA-256, SHA-384, SHA-512.
· RSA: 1024, 2048 bitů, 4096 bitů	ANO	· RSA: 1024, 2048 bitů, 4096 bitů
· Eliptické křivky: P-256, P-384, P-521	ANO	· Eliptické křivky: P-256, P-384, P-521
Dodané HW prostředky musí být plně otevřený i jiným systémům, jenž vydávají na takový HW obsah a to s otevřenou dokumentací pro další integrace.	ANO	Dodané HW prostředky musí být plně otevřený i jiným systémům, jenž vydávají na takový HW obsah a to s otevřenou dokumentací pro další integrace.
Dodané HW prostředky musí být plně funkční i po ukončení používání SW balíku pro centrální vydávání obsahu.	ANO	Dodané HW prostředky musí být plně funkční i po ukončení používání SW balíku pro centrální vydávání obsahu.

Kryptografický obsah čipové karty musí být logicky oddělen na část pro uložení komerčních certifikátů včetně šifrovacích klíčů (dále „komerčních ID“) a na samostatnou část pro uložení kvalifikovaných certifikátů a jim příslušných šifrovacích klíčů (dále „kvalifikovaných ID“).	ANO	Kryptografický obsah čipové karty musí být logicky oddělen na část pro uložení komerčních certifikátů včetně šifrovacích klíčů (dále „komerčních ID“) a na samostatnou část pro uložení kvalifikovaných certifikátů a jim příslušných šifrovacích klíčů (dále „kvalifikovaných ID“).
Výše zmíněné části musí být na sobě nezávislé. Tzn. jejich správa a přístupy včetně přístupových oprávnění musí být na sobě nezávislé.	ANO	Výše zmíněné části musí být na sobě nezávislé. Tzn. jejich správa a přístupy včetně přístupových oprávnění musí být na sobě nezávislé.
Přístup k části s komerčními ID musí být chráněn uživatelským heslem a administrátorským heslem. Tato hesla budou nezávislá (tj. oddělená) na uživatelském hesle a administrátorském hesle pro přístup do části s kvalifikovanými ID.	ANO	Přístup k části s komerčními ID musí být chráněn uživatelským heslem a administrátorským heslem. Tato hesla budou nezávislá (tj. oddělená) na uživatelském hesle a administrátorském hesle pro přístup do části s kvalifikovanými ID.
Z bezpečnostních důvodů je vyžadováno, aby čipová karta byla plně v souladu s “Security Target” vydaným výrobcem čipové karty. Cílem tohoto požadavku je vyloučení jakýchkoliv zásahů do obsahu, funkce či nastavení kryptografického čipu třetí stranou, které by mohly potenciálně zpochybnit shodu dodaných čipových karet s kartami výrobce, které prošly certifikací Common Criteria a jsou platně zapsány na evropský seznam QSCD prostředků.	ANO	Z bezpečnostních důvodů je vyžadováno, aby čipová karta byla plně v souladu s “Security Target” vydaným výrobcem čipové karty. Cílem tohoto požadavku je vyloučení jakýchkoliv zásahů do obsahu, funkce či nastavení kryptografického čipu třetí stranou, které by mohly potenciálně zpochybnit shodu dodaných čipových karet

		s kartami výrobce, které prošly certifikací Common Criteria a jsou platně zapsány na evropský seznam QSCD prostředků.
V rámci sjednoceného přihlašování (SSO) musí dodaný systém zajistit automatické přihlášení do stanice Windows 10/11:		V rámci sjednoceného přihlašování (SSO) musí dodaný systém zajistit automatické přihlášení do stanice Windows 10/11:
- Informační systém školy – studenti a zaměstnanci - Štefl software	ANO	- Informační systém školy – studenti a zaměstnanci - Štefl software
- Informační systém - Avensio - zpracování mezd - RSM Payroll Centre CZ s.r.o.	ANO	- Informační systém - Avensio - zpracování mezd - RSM Payroll Centre CZ s.r.o.
- Informační systém - Helios Fenix - Účetní software a evidence majetku	ANO	- Informační systém - Helios Fenix - Účetní software a evidence majetku
- Informační systém - Docházka (žáci + zaměstnanci), JobAbacusPro, GACC s. r. o	ANO	- Informační systém - Docházka (žáci + zaměstnanci), JobAbacusPro, GACC s. r. o
- Informační systém - EDUBAS	ANO	- Informační systém - EDUBAS
Systém musí dokázat vynutit a zajistit pro vybrané autorizované aplikace v rámci SSO další přihlašovací faktor pomocí passkeys,, T-OTP,.	ANO	Systém musí dokázat vynutit a zajistit pro vybrané autorizované aplikace v rámci SSO další přihlašovací faktor pomocí passkeys,, T-OTP,.
Požadavky na podporu	**ANO/NE**	**Popis splnění požadavku**
Podpora výrobce v režimu 8x5 pro platformu i její provozní konfiguraci včetně politik na 5 let	ANO	Podpora výrobce v režimu 8x5 pro platformu

		i její provozní konfiguraci včetně politik na 5 let

implementace

Nástroj pro ověřování identity uživatelů		
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
nastavení	ANO	nastavení
akceptační testy a testovací provoz	ANO	akceptační testy a testovací provoz
školení administrátorů v rozsahu 4 hodin	ANO	školení administrátorů v rozsahu 4 hodin
dokumentace skutečného provedení	ANO	dokumentace skutečného provedení

Tiskárna – potisk čipových karet

Nástroj pro ověřování identity uživatelů		
Název a výrobce	**Výrobce:Zebra** **Název: Printer ZC300**	
Požadovaný počet : 1		
Minimální technické požadavky	ANO/NE	Popis splnění požadavku
Velikost karty: CR-80, formát ISO 7810, typ ID-1	ANO	Velikost karty: CR-80, formát ISO 7810, typ ID-1
Tloušťka karty: 10 – 50 mil (0,25 – 1,27 mm)	ANO	Tloušťka karty: 10 – 50 mil (0,25 – 1,27 mm)
Tloušťka karty pro laminaci: 30 mil (0,76 mm)	ANO	Tloušťka karty pro laminaci: 30 mil (0,76 mm)
Tisková oblast na celou plochu karty CR-80 (bez okrajový tisk)	ANO	Tisková oblast na celou plochu karty CR-80 (bez okrajový tisk)
Rozlišení 300 DPI	ANO	Rozlišení 300 DPI
Barvy	ANO	Barvy
Rychlost tisku min 225 karet / hodina dual-sided printing	ANO	Rychlost tisku min 225 karet / hodina dual-sided printing
Kapacita vstupního zásobník 250 karet	ANO	Kapacita vstupního zásobník 250 karet
Kapacita výstupního zásobníku 100 karet	ANO	Kapacita výstupního zásobníku 100 karet
SW ovladače pro Windows® 10 / 11 / Server 2016 a vyšší	ANO	SW ovladače pro Windows® 10 / 11 / Server 2016 a vyšší
USB 2.0 a Ethernet rozhraní s interním tiskovým serverem	ANO	USB 2.0 a Ethernet rozhraní s interním tiskovým serverem
Požadavky na podporu	**ANO/NE**	**Popis splnění požadavku**
Podpora výrobce v režimu 8x5 pro platformu i její provozní konfiguraci včetně politik na 5 let	ANO	Podpora výrobce v režimu 8x5 pro platformu i její provozní konfiguraci včetně politik na 5 let

Doplňující požadavky zadavatele

Uchazeč bere na vědomí, **že součástí akceptace plnění jsou výsledky auditu**, který bude prověřovat, zda jím implementovaná bezpečnostní opatření jsou funkční. Uchazeč pak poskytne součinnost nebo napraví nalezené chyby vysoké závažnosti v implementaci technických opatření.

Součástí je zajištění instalace a konfigurace veškerých komponent v návaznosti na stávající infrastrukturu školy (tj. včetně dopravy, montáže, instalace a implementace do stávající IT infrastruktury) v sídle zadavatele.

Součástí instalace musí být i zaškolení IT administrátorů minimálně v rozsahu nutném pro samostatnou administraci všech komponent zakázky. Administrací se rozumí zejména: konfigurace, monitoring činnosti, aktualizace, řešení problémů, zálohování konfigurace.

Zákaznická dokumentace bude zahrnovat:

- popis všech prvků/zařízení,
- popis způsobu zálohy a obnovy konfigurace všech prvků/zařízení
- veškeré požadavky na zachování záruky/podpory (např. environmentální, kompatibilita, …)
- informaci o způsobu řešení servisních požadavků

Dodavatel do své nabídky zahrne veškerý instalační materiál a kabeláž nutnou plnohodnotnému zprovoznění dodané technologie jako logického a funkčního celku.

Dodavatel zajistí instalaci a konfiguraci dodaných HW a SW komponent v návaznosti na stávající infrastrukturu organizace, a to včetně instalace a implementace do stávající IT infrastruktury v sídle zadavatele:

- instalace zařízení do standardní RACK skříně 19“ 42U
- implementace Best Practice scénářů pro dané konfigurace
- kontroly kompatibility verzí ovladačů a firmware jednotlivých zařízení a jejich aktualizace
- registrace záruk u výrobců
- umístění do racku a zapojení kabeláže vč. jejího označení,
- inicializace a konfigurace všech dodaných zařízení
- nastavení IP adres
- nastavení vysoké dostupnosti
- konfiguraci datových prostor polí, integrace s hypervizorem, nastavení dohledu a instalace SW pro monitoring výkonu
- zapojení do stávající LAN

Maintenance

MAINTENANCE - (software maintenance) je proces pravidelného udržování, vylepšování a opravování softwarových aplikací po jejich prvotním vývoji a nasazení. Zadavatel v rámci stanovení nabídkové ceny nacení veškerou potřebnou maintenance k řádnému provozovaní dodaného řešení. Potřebnou maintenence dodavatel nacení po dobu udržitelnosti projektu 5 let. Maintenance bude dle povahy dodaného řešení pokrývat níže uvedené scénáře:

Korekční údržba: Oprava chyb a problémů, které se objeví po nasazení softwaru. To může zahrnovat opravy bezpečnostních zranitelností, chyb v kódu nebo jiné problémy, které ovlivňují funkčnost softwaru.
Adaptivní údržba: Úpravy a změny softwaru, aby zůstal kompatibilní s měnícím se prostředím. To může zahrnovat aktualizace pro nové operační systémy, hardware nebo jiné softwarové závislosti.
Perfekcionistická údržba: Vylepšení softwaru za účelem zvýšení jeho výkonu nebo použitelnosti. To může zahrnovat optimalizaci kódu, zlepšení uživatelského rozhraní nebo zavádění nových funkcí. Údržba softwaru je klíčová pro zajištění, že software zůstane funkční, bezpečný a relevantní i po dlouhou dobu po jeho původním nasazení.

Podmínky technické podpory (SLA)

Tento požadavek je součástí Servisu Díla. Podpora a servis pro dodaný HW a SW budou poskytovány po dobu udržitelnosti projektu (tj. 60 měsíců od předání díla), nebude-li dohodnuto smluvními stranami jinak – dodavatel bude kalkulovat pro základní technickou podporu **2 hodiny/měsíc**.

Bude zajištěna udržitelnost HW a SW včetně třetích stran, dodaných v rámci veřejné zakázky. Technická podpora a servis zařízení HW a SW budou realizovány dodavatelem, případně prostřednictvím odpovídajícího servisního kanálu výrobce.

Technická podpora a servis budou realizovány primárně vzdáleným připojením. Výjimku tvoří činnosti nerealizovatelné vzdáleným připojením a vynucují si realizaci v místě zadavatele.

Dále uvedené požadavky se neuplatní ve vztahu k HW, u kterých je výše v technické specifikaci stanoven speciální požadavek. Dodavatel se zavazuje poskytovat zadavateli služby v režimu 24x7 v minimálním rozsahu:

- telefonická hot-line podpora prostřednictvím přiděleného tel. kontaktu pro okamžitou komunikaci 24x7 pro kritické incidenty
- Služba HelpDesk umožní příjem požadavku na servisní zásah v českém jazyce prostřednictvím webového rozhraní v režimu 24x7 (s výjimkou předem nahlášených servisních zásahů při správě systému HelpDesk).
- telefonická, e-mailová a podpora prostřednictvím vzdáleného připojení bude k dispozici minimálně v pracovních dnech od 7 do 16 hod.
- diagnostika a odstraňování poruch systému
- profylaxe - preventivní prohlídka systému v rozsahu
- kontrola stavu nainstalovaných updatů a hotfixů

- kontrola a analýza chybových logů systémového SW, stejně tak aplikačního programového vybavení
- kontrola vytíženosti systémových zdrojů
- sběr zpětné vazby od administrátorů systému

Dodavatel se zavazuje zadavateli, že jakékoliv vady plnění Servisu díla či jeho části, budou odstraněny na náklady dodavatele. Zadavatel bude incident oznamovat dodavateli bez zbytečného odkladu jedním ze způsobů a na kontaktních místech, kam budou mít zajištěny přístup pověřené osoby Zadavatele (HelpDesk).
Součástí nahlášení požadavku Zadavatelem musí být:

- popis Incidentu nebo Požadavku,
- jiné relevantní upřesňující informace, včetně případných textových či obrazových příloh nezbytných pro replikaci incidentu,
- kontaktní osoba.

Dodavatelem používaný systém pro HelpDesk musí pokrýt uvedené informace pro nahlášení požadavku. Dodavatel garantuje zadavateli čas pro odezvu a čas pro vyřešení provozního incidentu, a to pro jednotlivé kategorie provozních incidentů následovně:

Kategorie incident	Lhůta odezvy (IRT)	Lhůta vyřešení (TRT)
Kritický	60 minut	12 hodin
Závažný	60 minut	2 dny
Běžný	1 den	7 dní
Minoritní	3 dny	Best effort

Podpora je poskytovaná v českém jazyce ve formě Help-desk podpory a v případě kritického incidentu telefonické podpory. Jednotlivé úkony/akce dle specifikace podpory jsou definovány následovně.

Lhůta odezvy (IRT)

Je definovaná jako časový interval měřený od doby, kdy zadavatel ohlásil incident do Helpdeskové aplikace poskytovatele nebo telefonicky s následným zadáním do Helpdeskové aplikace po dobu, kdy je zpětně kontaktovaný dodavatelem nebo je incident přijat do řešení. Lhůta odezvy může být také označována jako reakční doba.

Doba vyřešení (TRT)

Je definovaná jako časový interval měřený od doby, kdy zadavatel ohlásil incident do Helpdeskové aplikace poskytovatele nebo telefonicky s následným zadáním do Helpdeskové aplikaci po dobu, kdy dodavatel vyřešil popsaný incident.

Priority

Zaručená lhůta odezvy na vzniklé incidenty se dělí dle jejich priority. Priorita je dána kritičností vzniklého incidentu v návaznosti na požadovanou funkčnost produktu:

- Kritický incident – Nefunkčnost způsobená dodanou technologií, Nefunkčnost/nedostupnost řešení

- Závažný incident – Nefunkčnost některé z komponent, která nedovoluje vykonávat požadovanou činnost. Vážné chyby řešení ovlivňující provoz objednatele.
- Běžný incident – Nefunkčnost některé z komponent, která nemá přímý dopad na dostupnost objednatele, vážné konfigurační chyby.
- Minoritní incident – Chyby v konfiguraci, Chyby řešení neovlivňující provoz objednatele, Nefunkčnost komponent minoritního charakteru.

Dodavatel neprodleně potvrdí obdržení požadavku v systému HelpDesk a poskytne Zadavateli informace o předpokládaném způsobu řešení požadavku, požadavcích na součinnost Zadavatele a předpokládaný termín vyřešení požadavku.

Dodavatel v průběhu řešení požadavku, pokud mu to charakter požadavku a způsob řešení umožňuje, průběžně informuje Zadavatele o aktuálním stavu a případných změnách v předpokládaném způsobu, požadované součinnosti a termínů vyřešení. V případě že dodavatel v průběhu řešení požadavku zjistí, že se jedná o Incident, jehož zdroj je prvek třetích stran, informuje Zadavatele o této skutečnosti, předpokládaném způsobu, požadované součinnosti a termínů vyřešení a pokračuje v řešení v režimu BE (Best Effort) tzn. dodavatel vyvine maximální možné úsilí na provedení požadavku a zejména na zajištění požadovaných parametrů předmětu plnění v nejkratší možné době.

Zjistí-li dodavatel v průběhu řešení Incidentu, že Incident je neodstranitelný, je v rámci Běžné pracovní doby povinen nepřetržitě pracovat na náhradním řešení a informovat o tomto stavu Zadavatele.

Zjistí-li dodavatel v průběhu řešení Incidentu, že Incident má přímou souvislost s neodborným či neoprávněným jednáním osob Zadavatele případně byl Incident vyvolán produkty či službami třetí osoby, je dodavatel povinen bezodkladně informovat o tomto stavu Zadavatele. Zadavatel se zavazuje bezodkladně uhradit v plné výši náklady nad rámec této smlouvy dodavatelem prokazatelně vynaložené k řešení Incidentu, přičemž samotná identifikace Incidentu je součástí plnění této smlouvy.

Zadavatel je oprávněn dořešení Incidentu kdykoliv zastavit či pozastavit, přičemž nárok dodavatele na úhradu již vynaložených prostředků zůstává nedotčen. Incident je v tomto případě považován za vyřešený.

V případě úspěšného vyřešení požadavku, je řešitel před ukončením požadavku povinen provést ověření funkčnosti služby (pokud je to možné). Iniciátora Incidentu informuje o:

- v případě Incidentu specifikuje příčinu (pokud je známa),
- vyzve iniciátora k ověření funkčnosti služby.

Po ověření funkčnosti ze strany Zadavatele se Požadavek považuje za vyřešený.

Po vyřešení požadavku dodavatel požadavek uzavře v systému HelpDesk a informuje Zadavatele.

Zadavatel má právo ve lhůtě deseti (10) dnů od uzavření požadavku vznést výhrady nebo připomínky ke způsobu řešení nebo k výslednému stavu; v takovém případě se požadavek nepovažuje za uzavřený a Strany se zavazují zahájit společné jednání za účelem odstranění

veškerých vzájemných rozporů a nalezení shody nad způsobem řešení nebo výsledném stavu, a to nejpozději do pěti (5) pracovních dnů od výzvy kterékoliv Strany.

Záruky na servisní služby

Zadavatel požaduje záruku na veškeré servisní služby provedené v rámci podpory provozu v délce trvání minimálně 3 měsíců (není-li u konkrétní služby uvedeno jinak) od okamžiku realizace. Veškeré HW opravy po dobu záruky budou bez dalších nákladů pro provozovatele.

Podmínky rozvoje řešení

V rámci části rozšířené servisní podpory (Služby rozvoje) je požadován rozvoj a údržba díla, tedy činnosti, které nejsou součástí SLA podpory. Cena za Služby rozvoje je pro účely porovnatelnosti nabídek vypočtena jako součin Ceny za jednu hodinu práce (implementace) bez DPH a předpokládaného rozsahu 100 hodin za období 5 let. Předpokládaný počet hodin je stanoven pouze pro účely hodnocení nabídek v zadávacím řízení. Zadavatel není povinen předpokládaný počet hodin služeb rozvoje vyčerpat.

Zajištění kybernetické bezpečnosti VOŠZ Brno - opakovaná

Zadavatel:	**Vyšší odborná škola zdravotnická Brno, příspěvková organizace**
Dodavatel:	**Aricoma Systems a.s.**
Datum vyplnění:	**18.08.2025**

Cena za jeden člověkoden práce (implementace) bez DPH: 15 000 Kč

Dílo							
Aktivita	**Počet člověkodní implementace**	**Cena implementace bez DPH**	**Cena HW, SW vč. záruky na 3 roky bez DPH**	**Cena za dodávku a implementaci řešení vč. standardní záruky (3 roky) bez DPH**	**Cena za poskytnutí nadstandardní (prodloužené) záruky pro 4. a 5. rok plnění bez DPH**	**Cena full maintenance na 5 let s DPH**	
ID001 - ZABEZPEČENÍ SÍŤOVÉ INFRASTRUKTURY (NAC/802.1X) + ZABEZPEČENÍ PERIMETRU NGFW	30	450 000,00 Kč	**2 425 000,00 Kč**	2 875 000,00 Kč	18 000,00 Kč	21 780,00 Kč	
ID002 - Zvýšení redundance a zabezpečení primárního datového centra	20	300 000,00 Kč	**1 999 000,00 Kč**	2 299 000,00 Kč	5 000,00 Kč	6 050,00 Kč	
ID003 - OCHRANA KONCOVÝCH STANIC ENDPOINt	10	150 000,00 Kč	**732 000,00 Kč**	882 000,00 Kč	0,00 Kč	0,00 Kč	Záruka irelevantní, jedna se o SW, vše v maintenance
ID004 - ANALÝZA SÍŤOVÉHO PROVOZU (OCHRANA INTEGRITY SÍTĚ ŠKOLY)	10	150 000,00 Kč	**1 050 000,00 Kč**	1 200 000,00 Kč	6 800,00 Kč	8 228,00 Kč	
ID005 - MFA + SSO OCHRANA IDENTITY UŽIVATELŮ	40	600 000,00 Kč	**2 800 000,00 Kč**	3 400 000,00 Kč	12 500,00 Kč	15 125,00 Kč	
SUMA	**110**	**1 650 000,00 Kč**	**9 006 000,00 Kč**	**10 656 000,00 Kč**	**42 300,00 Kč**	**51 183,00 Kč**	

Servis			
Kategorie	**Cena za 1 rok bez DPH**	**Cena za 5 let bez DPH**	**Cena za 5 let s DPH**
Plná údržba řešení (Full maintenance)	8 460,00 Kč	42 300,00 Kč	51 183,00 Kč
Technická podpora dodavatele v režimu 24-7 (SLA) *	180 000,00 Kč	900 000,00 Kč	1 089 000,00 Kč
SUMA	**188 460,00 Kč**	**942 300,00 Kč**	**1 140 183,00 Kč**

Rozšířená technická podpora			
Kategorie	**Cena za HODINOVOU SAZBU bez DPH**	**Počet H/5 let/ bez DPH**	**Počet MD/5 let/ s DPH**
Služby rozvoje - Rozšířená technická podpora **	2 000,00 Kč	200 000,00 Kč	242 000,00 Kč
SUMA		**200 000,00 Kč**	**242 000,00 Kč**

Sumarizace	**Cena bez DPH**	**Cena s DPH**
ID001 - Zabezpečení síťové infrastruktury (NAC/802.1x) + Zabezpečení perimetru NGFW	**2 875 000,00 Kč**	**3 478 750,00 Kč**
ID002 - Zvýšení redundance a zabezpečení primárního datového centra	**2 299 000,00 Kč**	**2 781 790,00 Kč**
ID003 - Ochrana koncových stanic ENDPOINT	**882 000,00 Kč**	**1 067 220,00 Kč**
ID004 - Analýza síťového provozu (ochrana integrity sítě školy)	**1 200 000,00 Kč**	**1 452 000,00 Kč**
ID005 - MFA + SSO ochrana identity uživatelů	**3 400 000,00 Kč**	**4 114 000,00 Kč**
Celková cena díla	**10 656 000,00 Kč**	**12 893 760,00 Kč**
Celková cena servisu	**942 300,00 Kč**	**1 140 183,00 Kč**
Celková cena	**11 598 300,00 Kč**	**14 033 943,00 Kč**

Sumarizace	**Cena bez DPH**	**Cena s DPH**
Cena za dodávku a implementaci řešení vč. standardní záruky	**10 656 000,00 Kč**	**12 893 760,00 Kč**
Cena za poskytnutí nadstandardní (prodloužené) záruky pro 4. a 5. rok plnění	42 300,00 Kč	51 183,00 Kč
tj. roční plnění (12 měsíců) činí	**21 150,00 Kč**	**25 591,50 Kč**
Cena za poskytnutí potřebné maintenance support a Základní technické podpory na 5 let	**942 300,00 Kč**	**1 140 183,00 Kč**
tj. roční plnění maintenance support (12 měsíců)	**8 460,00 Kč**	**10 236,60 Kč**
tj. roční plnění základní tech. podpory (12 měsíců) činí	**180 000,00 Kč**	**217 800,00 Kč**
Cena za poskytnutí rozšířené servisní podpory na 5 let (předpokládaná kalkulace 100 hodin)	**200 000,00 Kč**	**242 000,00 Kč**
cena za 1 hodinu služeb rozšířené servisní podpory činí)	**2 000,00 Kč**	**2 420,00 Kč**
CELKOVÁ CENA - kritérium hodnocení (k doplnění do čl. VI. odst. 1. Smlouvy)	**11 798 300,00 Kč**	**14 275 943,00 Kč**

Nabídková cena:
musí být v nabídce doložena položkovým rozpočtem, který je součástí tohoho dokumentu . Hodnoty uvedené v položkovém rozpočtu považuje zadavatel za závazné pro účely plnění veřejné zakázky; odpovědnost za soulad součtu položkových cen a celkové nabídkové ceny nese účastník,

musí zahrnovat veškeré náklady vzniklé v souvislosti s plněním veřejné zakázky; součástí nabídkové ceny jsou veškeré práce, dodávky, poplatky a jiné náklady účastníka nezbytné pro řádné a úplné provedení předmětu plnění, není-li zadávacími podmínkami výslovně stanoveno jinak

může být měněna pouze za podmínek vyplývajících ze zadávací dokumentace, jsou-li takové podmínky dány.

Dodavatel doplní do položkového rozpočtu Název a výrobce uvedfený v příoze č.01_Technická specifikace plnění a doplní jeho PartNumber (je-li známo)
Dodavatel ve sloupci Typ a Aktivita (ID00x) vyplní položku z uvedeného výběru.

Technická podpora dodavatele v režimu 24-7 (SLA) *
Základní technická podpora (ZTP) - uchazeč nacení základní technickou podporu poskytovanou formou servisních služeb v časové dotaci: **2HOD x 12 měsíců** . Uchazeč do jednotkové ceny uvede celkový počet hodin/rok **za základní technickou podporu**

Služby rozvoje - Rozšířená technická podpora **
Rozšířená servisní podpora - uchazeč nacení rozšířenou technickou podporu, která bude čerpána na základě požadavku zadavatele a účtována dle její spotřeby nad rámec základní servisní podpory. Uchazeč nacení hodinovou sazbu. Tato hodinová sazba bude fixní po celou dobu poskytování RSP. Pro potřeby hodnocení bude kalkulován předpokládaný počet **100 hodin / 5let** rozšířené technické podpory. Uchazeč do jednotkové ceny uvede nabízenou **HODINOVOU SAZBU**

#	PartNumber	Výrobce	Popis/Název	Typ	Aktivita (ID00x)	Jednotková nabídková cena za 1ks v Kč bez DPH	Nabízený počet kusů celkem	Celková výše nabídkové ceny za všechny kusy v Kč bez DPH
1	CUSTOM	FORTINET	Výrobce: Fortinet Název: FortiGate 91G + UTP Výrobce: FORTINET Název: FortiSwitch-624F + 5 Year FortiCare Premium Support Výrobce: FORTINET Název: FortiSwitch-148F-FPOE + 5 Year FortiCare Premium Support Výrobce: FORTINET Název: FortiSwitch-124F-FPOE + 5 Year FortiCare Premium Support 10G SFP+ Výrobce: FORTINET Název: FortiAP-231K+ 5 Year FortiCare Premium Support Výrobce: FORTINET Název: FortiNAC Control and Application Extended-VM + FortiCare Premium Support Výrobce: FORTINET Název: FortiAnalyzer-VM Subscription License with Support	HW+SW	ID001 - ZABEZPEČENÍ SÍŤOVÉ INFRASTRUKTURY (NAC/802.1X) + ZABEZPEČENÍ PERIMETRU NGFW	2 875 000,00 Kč	1	2 875 000,00 Kč
2	CUSTOM	DELL, SYNOLOGY, VEEAM, APC, MICROSOFT	Výrobce DELL Název: SERVER DELL PowerEdge R760 – konfigurace plnící všechny min. tech specifikace Výrobce DELL Název: SERVER DELL PowerEdge R760 – konfigurace plnící všechny min. tech specifikace Výrobce DELL Název: SERVER DELL PowerEdge R760 – konfigurace plnící všechny min. tech specifikace Výrobce DELL Název: Dell ME5024 Storage – konfigurace plnící všechny min. tech specifikace Výrobce: Synology Název: NAS RS1221+ Rack Station (plnící všechna min parametry) + 4x Synology HAT5300/16TB/HDD/3.5"/SATA/7200 RPM/SR Výrobce: APC Název: APC Smart-UPS 3000VA LCD RM 2U 230V with SmartConnect Výrobce: VEEAM Název: Veeam Data Platform Essentials Universal Subscription License. Includes Enterprise Plus Edition features. CSP Windows Server 2022 - 1 Device CAL EDU - 200x CSP Windows Server 2022 Remote Desktop Services - 1 User CAL EDU - 15x CSP Windows Server 2022 Datacenter - 16 Core EDU - 4x	HW+SW	ID002 - Zvýšení redundance a zabezpečení primárního datového centra	2 299 000,00 Kč	1	2 299 000,00 Kč
3	CUSTOM	ESET	Výrobce. ESET Název: PROTECT ELITE	Licence	ID003 - OCHRANA KONCOVÝCH STANIC ENDPOINt	882 000,00 Kč	1	882 000,00 Kč
4	CUSTOM	GREYCORTEX	Výrobce: GREYCORTEX Typ: Mendel AIO	HW+SW	ID004 - ANALÝZA SÍŤOVÉHO PROVOZU (OCHRANA INTEGRITY SÍTĚ ŠKOLY)!!	1 200 000,00 Kč	1	1 200 000,00 Kč
5	CUSTOM	GITRIX, ZEBRA	Výrobce: Gitrix Název: GITRIX Výrobce:Zebra Název: Printer ZC300	HW+SW	ID005 - MFA + SSO OCHRANA IDENTITY UŽIVATELŮ	3 400 000,00 Kč	1	3 400 000,00 Kč
6								0,00 Kč
7								0,00 Kč
8								0,00 Kč
9								0,00 Kč
10								0,00 Kč
11								0,00 Kč
12								0,00 Kč
13								0,00 Kč
14								0,00 Kč
15								0,00 Kč
16								0,00 Kč
17								0,00 Kč
18								0,00 Kč
19								0,00 Kč
20								0,00 Kč
21								0,00 Kč
22								0,00 Kč
23								0,00 Kč
24								0,00 Kč
25								0,00 Kč
26								0,00 Kč
27								0,00 Kč
28								0,00 Kč
29								0,00 Kč
30								0,00 Kč
31								0,00 Kč
32								0,00 Kč
33								0,00 Kč
34								0,00 Kč
35								0,00 Kč
36								0,00 Kč
37								0,00 Kč
38								0,00 Kč
39								0,00 Kč
40								0,00 Kč
41								0,00 Kč
42								0,00 Kč
43								0,00 Kč
44								0,00 Kč
45								0,00 Kč
46								0,00 Kč
47								0,00 Kč
48								0,00 Kč
49								0,00 Kč
50								0,00 Kč
51								0,00 Kč
52								0,00 Kč
53								0,00 Kč
54								0,00 Kč
55								0,00 Kč
56								0,00 Kč
57								0,00 Kč
58								0,00 Kč
59								0,00 Kč
60								0,00 Kč
61								0,00 Kč
62								0,00 Kč
63								0,00 Kč
64								0,00 Kč
65								0,00 Kč
66								0,00 Kč
67								0,00 Kč
68								0,00 Kč
69								0,00 Kč
70								0,00 Kč
71								0,00 Kč
72								0,00 Kč
73								0,00 Kč
74								0,00 Kč
75								0,00 Kč
76								0,00 Kč
77								0,00 Kč
78								0,00 Kč
79								0,00 Kč
80								0,00 Kč
81								0,00 Kč
82								0,00 Kč
83								0,00 Kč
84								0,00 Kč
85								0,00 Kč
86								0,00 Kč
87								0,00 Kč
88								0,00 Kč
89								0,00 Kč
90								0,00 Kč
91								0,00 Kč
92								0,00 Kč
93								0,00 Kč
94								0,00 Kč
95								0,00 Kč
96								0,00 Kč
97								0,00 Kč
98								0,00 Kč
99								0,00 Kč
100								0,00 Kč
101								0,00 Kč
102								0,00 Kč
103								0,00 Kč
104								0,00 Kč
105								0,00 Kč
106								0,00 Kč
107								0,00 Kč
108								0,00 Kč
109								0,00 Kč
110								0,00 Kč
111								0,00 Kč
112								0,00 Kč
113								0,00 Kč
114								0,00 Kč
115								0,00 Kč
116								0,00 Kč
117								0,00 Kč
118								0,00 Kč
119								0,00 Kč
120								0,00 Kč
121								0,00 Kč
122								0,00 Kč
123								0,00 Kč
124								0,00 Kč
125								0,00 Kč
126								0,00 Kč
127								0,00 Kč
128								0,00 Kč
129								0,00 Kč
130								0,00 Kč
131								0,00 Kč
132								0,00 Kč
133								0,00 Kč
134								0,00 Kč
135								0,00 Kč
136								0,00 Kč
137								0,00 Kč
138								0,00 Kč
139								0,00 Kč
140								0,00 Kč
141								0,00 Kč
142								0,00 Kč

143								0,00 Kč
144								0,00 Kč
145								0,00 Kč
146								0,00 Kč
147								0,00 Kč
148								0,00 Kč
149								0,00 Kč
150								0,00 Kč
151								0,00 Kč
152								0,00 Kč
153								0,00 Kč
154								0,00 Kč
155								0,00 Kč
156								0,00 Kč
157								0,00 Kč
158								0,00 Kč
159								0,00 Kč
160								0,00 Kč
161								0,00 Kč
162								0,00 Kč
163								0,00 Kč
164								0,00 Kč
165								0,00 Kč
166								0,00 Kč
167								0,00 Kč
168								0,00 Kč
169								0,00 Kč
170								0,00 Kč
171								0,00 Kč
172								0,00 Kč
173								0,00 Kč
174								0,00 Kč
175								0,00 Kč
176								0,00 Kč
177								0,00 Kč
178								0,00 Kč
179								0,00 Kč
180								0,00 Kč
181								0,00 Kč
182								0,00 Kč
183								0,00 Kč
184								0,00 Kč
185								0,00 Kč
186								0,00 Kč
187								0,00 Kč
188								0,00 Kč
189								0,00 Kč
190								0,00 Kč
191								0,00 Kč
192								0,00 Kč
193								0,00 Kč
194								0,00 Kč
195								0,00 Kč
196								0,00 Kč
197								0,00 Kč
198								0,00 Kč
	Celková cena za dílo							10 656 000,00 Kč

* Celková cena za dílo musí být shodná s Cenou za dodávku a implementaci řešení vč. standardní záruky uvedenou v listě s názvem "Cenová nabídka" v buňce C41.

Příloha č. 3 smlouvy

Realizační tým

Projektový manažer – Filip Junga

Technický specialista – Mrkvica Stanislav

Specialista/konzultant – kybernetická bezpečnost – Chalota Jiří

Doklady realizačního týmu jsou součástí nabídky.

Příloha č. 4 smlouvy

Seznam poddodavatelů

K plnění veřejné zakázky nebudou využití žádní poddodavatelé – Dodavatel bude zakázku realizovat výhradně vlastními silami.